CFRG
Research Group Status

IETF 118 Prague

Chairs:

Stanislav Smyshlyaev <smyshsv@gmail.com>

Nick Sullivan <nicholas.sullivan@gmail.com>

Alexey Melnikov <alexey.melnikov@isode.com>

Administrative

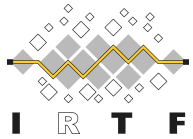
- This session is being recorded
- Minute taker in HedgeDoc
- Jabber comment relay

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

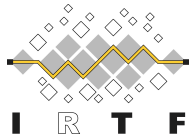
Minutes: **https://notes.ietf.org/notes-ietf-118-cfrg**

Note Well – Intellectual Property



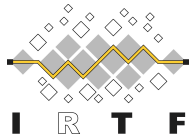
- **The IRTF follows the IETF Intellectual Property Rights (IPR) disclosure rules**
- By participating in the IRTF, you agree to follow IRTF processes and policies:
  - If you are aware that any IRTF contribution is covered by patents or patent applications that are owned or controlled by you or your 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/118/session/cfrg

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

Agenda

https://datatracker.ietf.org/meeting/118/session/cfrg

Chairs: Stanislav Smyshlyaev, Nick Sullivan and Alexey Melnikov

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

15:05 - Chris Patton, "VDAF" (10+5 mins)

15:20 - Vasilis Kalos, "The BBS Signature Scheme" (10+5 mins)

15:35 - Andrey Bozhko, "Properties of AEAD algorithms" (5+5 mins)

15:45 - Alexander Dax, "How Subtle AEAD Differences can Impact Protocol Security" (10+5 mins)

16:00 - Dimitris Mouris, "The Mastic VDAF" (10+3 mins)

16:13 - Hubert Kario, "Implementation Guidance for the PKCS #1 RSA Cryptography Specification" (10+3 mins)

16:26 - David Joseph, "Batched Signatures" (4 mins)

RG Document Status

Document Status (1 of 3)

- New RFC (since July)
  - RFC 9380 (draft-irtf-cfrg-hash-to-curve): Hashing to Elliptic Curves
  - RFC 9381 (draft-irtf-cfrg-vrf): Verifiable Random Functions (VRFs)
  - RFC 9382 (draft-irtf-cfrg-spake2): SPAKE2, a Password-Authenticated Key Exchange
  - RFC 9474 (draft-irtf-cfrg-rsa-blind-signatures): RSA Blind Signatures
- In RFC Editor's queue
  - draft-irtf-cfrg-voprf-21 (**AUTH48**): Oblivious Pseudorandom Functions (OPRFs) using Prime-Order Groups
  - draft-irtf-cfrg-ristretto255-decaf448-08 (**AUTH48**): The ristretto255 and decaf448 Groups
- In IESG review
  - draft-irtf-cfrg-frost-15 (**updated**): FROST: Flexible Round-Optimized Schnorr Threshold Signatures
- In IRSG review
  - None
- Waiting for IRTF Chair
  - None

Document Status (2 of 3)

- Active CFRG drafts
  - draft-irtf-cfrg-kangarootwelve-11 (**waiting for chairs to review second RGLC outcome**): KangarooTwelve eXtendable Output Function
  - draft-irtf-aegis-aead-06 (**updated**): The AEGIS family of authenticated encryption algorithms
  - draft-irtf-cfrg-bbs-signatures-04 (**updated**): The BBS Signature Scheme
  - draft-irtf-cfrg-dnhpke-03 (**updated**): Deterministic Nonce-less Hybrid Public Key Encryption
  - draft-irtf-cfrg-aead-properties-02 (**updated**): Properties of AEAD algorithms
  - draft-irtf-cfrg-aead-limits-07: Usage Limits on AEAD Algorithms
  - draft-irtf-cfrg-opaque-12 (**updated**): The OPAQUE Asymmetric PAKE Protocol
  - draft-irtf-cfrg-cpace-10 (**updated**): CPace, a balanced composable PAKE
  - draft-fluhrer-lms-more-parm-sets-11 (**updated**): Additional Parameter sets for LMS Hash-Based Signatures
  - draft-irtf-cfrg-vdaf-07 (**updated**): Verifiable Distributed Aggregation Functions
  - draft-irtf-cfrg-signature-key-blinding-04 (**updated**): Key Blinding for Signature Schemes

Document Status (3 of 3)

- Recently adopted documents
  - draft-irtf-cfrg-cryptography-specification-00: Guidelines for Writing Cryptography Specifications
- 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-bls-signature-05**: BLS Signatures
  - **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-hoffman-c2pq-07: The Transition from Classical to Post-Quantum Cryptography

AOB