CFRG Research Group

Online Agenda and Slides at:

https://datatracker.ietf.org/doc/agenda-105-cfrg/

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

Agenda

https://datatracker.ietf.org/doc/agenda-105-cfrg/

IETF Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.
As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF 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.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

As a reminder:

- 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.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process),
- BCP 25 (Working Group processes),
- BCP 25 (Anti-Harassment Procedures),
- BCP 54 (Code of Conduct),
- BCP 78 (Copyright),
- BCP 79 (Patents, Participation),
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

Administrative

- Audio Streaming/Recording
  - Please speak only using the microphones
  - Please state your name before speaking

- Minute takers & Etherpad
- Jabber

CFRG Research Group Status

Chairs:

Kenny Paterson <kenny.paterson@inf.ethz.ch>

Alexey Melnikov <alexey.melnikov@isode.com>

Nick Sullivan <nick@cloudflare.com>

RG Document Status

Document Status

- New RFC (since Prague)
  - RFC 8554 (**document shepherd: Paul Hoffman**): Hash-Based Signatures
  - RFC 8452: AES-GCM-SIV: nonce misuse-resistant authenticated encryption
- In RFC Editor's queue (since Prague)
  - draft-irtf-cfrg-re-keying-17: Re-keying Mechanisms for Symmetric Keys
- In IRSG review
  - draft-irtf-cfrg-argon2-06 (**updated**, **almost ready for IRSG, some comments from IRTF Chair to address**): memory-hard Argon2 password hash and proof-of-work function
- Completed, waiting for chairs
  - draft-irtf-cfrg-spake2-08 (**waiting for shepherd's review** (Kenny)): SPAKE2, a PAKE
- Active CFRG drafts
  - draft-irtf-cfrg-hash-to-curve-04 (**updated**): Hashing to Elliptic Curves
  - draft-irtf-cfrg-vrf-04: Verifiable Random Functions (VRFs)
  - draft-irtf-cfrg-randomness-improvements-06 (**updated, RGLC**): Randomness Improvements for Security Protocols
  - draft-viguier-kangarootwelve-04: KangarooTwelve eXtendable Output Function
  - draft-irtf-cfrg-xchacha-00 (**updated**): XChaCha: eXtended-nonce ChaCha and AEAD_XChaCha20_Poly1305
  - draft-irtf-cfrg-voprf-00 (**newly adopted work item, updated**): Oblivious Pseudorandom Functions (OPRFs) using Prime-Order Groups
  - draft-irtf-cfrg-hpke-00 (**newly adopted work item, updated**): Hybrid Public Key Encryption
  - draft-boneh-bls-signature-00 (**newly adopted work item**): BLS Signature Scheme
- Related work/possible work item
  - draft-hoffman-c2pq-05 (**updated**): The Transition from Classical to Post-Quantum Cryptography
  - draft-hoffman-rfc6090bis-02: Fundamental Elliptic Curve Cryptography Algorithms
- 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)

Crypto Review Panel

- Formed in September 2016
  - Wiki page for the team: <https://trac.ietf.org/trac/irtf/wiki/Crypto%20Review%20Panel>
- May be used to review documents coming to CFRG, Security Area or Independent Stream.
- **Lots of good reviews done!**
- CFRG chairs would rely on help from the Crypto Review Panel to review PAKE candidates.
- Membership extended till the end of December 2019 (initial term 2 years).
- **Chairs are looking for new members, please submit your nominations to cfrg-chairs@ietf.org before September 1st 2019. Self nominations are welcome.**

PAKE selection process

- Nomination period ended in June
- Information about submissions (e.g. RFC 8125 compliance) was sent by authors/nominees
  - The aim is to select 0 or more PAKE to recommend to the wider IETF community
- Stanislav is going to present summary at the end of this section
- Suggestions on how to pick the best PAKE are very welcome! Which questions should CFRG chairs ask?

AOB