CFRG Research Group

Online Agenda and Slides at:
https://datatracker.ietf.org/meeting/94/agenda/cfrg/

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

https://datatracker.ietf.org/meeting/95/agenda/cfrg/
This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

**The brief summary:**

- By participating with the IETF, you agree to follow IETF processes.
- If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.
- You understand that meetings might be recorded, broadcast, and publicly archived.

For further information, talk to a chair, ask an Area Director, or review the following:

- BCP 9 (on the Internet Standards Process)
- BCP 25 (on the Working Group processes)
- BCP 78 (on the IETF Trust)
- BCP 79 (on Intellectual Property Rights in the IETF)

Also see: [http://www.ietf.org/about/note-well.html](http://www.ietf.org/about/note-well.html)
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@rhul.ac.uk>
Alexey Melnikov <alexey.melnikov@isode.com>
RG Document Status
Document Status

• New RFC
  – RFC 7664 - Dragonfly Key Exchange
  – RFC 7748 - Elliptic Curves for Security

• In RFC Editor's queue
  – None

• Completed, waiting for chairs
  • draft-irtf-cfrg-eddsa-05: Edwards-curve Digital Signature Algorithm (EdDSA) - complete, chairs need to do final sanity check and request IRSG review.

• Active CFRG drafts
  • draft-irtf-cfrg-xmss-hash-based-signatures-03 (updated): XMSS: Extended Hash-Based Signatures - in RGLC
  • draft-mcgrew-hash-sigs-04 (updated): Hash-Based Signatures
  • draft-irtf-cfrg-pake-reqs-02 (updated): Requirements on PAKE schemes - ready for RGLC.
  • draft-irtf-cfrg-spake2-03 (updated): SPAKE2, a PAKE
  • draft-irtf-cfrg-augpake-05 (updated): Augmented Password-Authenticated Key Exchange (AugPAKE)
  • draft-irtf-cfrg-argon2-00 (new): The memory-hard Argon2 password hash and proof-of-work function

• Related work/possible work item
  • AES-GCM-SIV call for adoption
  • draft-hoffman-rfc6090bis-02: Fundamental Elliptic Curve Cryptography Algorithms

• Expired
  – draft-irtf-cfrg-cipher-catalog-01: Ciphers in Use in the Internet
Crypto Review Team

- Suggested by Stephen Farrell (Sec AD)
- May be used to review documents coming to CFRG, Security Area or Independent Stream