CFRG Research Group

Online Agenda and Slides at:

https://datatracker.ietf.org/meeting/90/agenda/cfrg/

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

Agenda

http://www.ietf.org/proceedings/90/agenda/agenda-90-cfrg

IETF Note Well

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:

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:

Kevin Igoe <kmigoe@nsa.gov>

Kenny Paterson <kenny.paterson@rhul.ac.uk>

Alexey Melnikov <alexey.melnikov@isode.com>

RG Document Status

Document Status

- Published
  - RFC 7253 - The OCB Authenticated-Encryption Algorithm
- New document accepted as a work item
  - draft-nir-cfrg-chacha20-poly1305-06
- Post RG LC, chairs reviewing status
  - draft-irtf-cfrg-dragonfly-04
- Expired, talking to editors
  - draft-irtf-cfrg-cipher-catalog-01: Ciphers in Use in the Internet
- Active, chairs need to review status
  - draft-irtf-cfrg-augpake-01: Augmented Password-Authenticated Key Exchange (AugPAKE)
- Related work/possible work item
  - draft-hoffman-rfc6090bis-00: Fundamental Elliptic Curve Cryptography Algorithms

Work Item: New Curves for TLS

- CFRG has been asked to recommend new elliptic curves for use in TLS by the TLS WG.
- Curves suitable for use for both key establishment and digital signature.
- One curve or set of curves at each of 128-bit, 256-bit security levels; 192-bit security optional.
- This will be a major work item for CFRG over the next few months.

AOB

- Request from W3C