CFRG Research Group

Online Agenda and Slides at:

https://datatracker.ietf.org/meeting/93/agenda/cfrg/

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

Agenda

https://datatracker.ietf.org/meeting/93/agenda/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:

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

Alexey Melnikov <alexey.melnikov@isode.com>

RG Document Status

Document Status

- New RFC
  - draft-irtf-cfrg-chacha20-poly1305-10 was published as RFC 7539!
- In IESG for review for conflicts with IETF work
  - draft-irtf-cfrg-dragonfly-08
- Active CFRG drafts
  - draft-irtf-cfrg-pake-reqs-00: Requirements on PAKE schemes
  - draft-irtf-cfrg-spake2-01: SPAKE2, a PAKE
  - draft-irtf-cfrg-augpake-03: Augmented Password-Authenticated Key Exchange (AugPAKE)
  - draft-irtf-cfrg-xmss-hash-based-signatures-01: XMSS: Extended Hash-Based Signatures
- Expired
  - draft-irtf-cfrg-cipher-catalog-01: Ciphers in Use in the Internet
- 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.
- We decided on 2 curves: 25519 and Goldilocks.
- We need to decide on signatures (5 proposals)

AOB