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/94/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
  - None since Prague IETF
- In RFC Editor's queue
  - draft-irtf-cfrg-dragonfly-08 (in AUTH48)
  - draft-irtf-cfrg-curves-11 (**finally**!)
- Active CFRG drafts
  - draft-irtf-cfrg-eddsa-00 (**new draft**): Edwards-curve Digital Signature Algorithm (EdDSA)
  - draft-irtf-cfrg-pake-reqs-01 (**updated**): Requirements on PAKE schemes
  - draft-irtf-cfrg-spake2-02 (**updated**): SPAKE2, a PAKE
  - draft-irtf-cfrg-augpake-04: Augmented Password-Authenticated Key Exchange (AugPAKE)
  - draft-irtf-cfrg-xmss-hash-based-signatures-01: XMSS: Extended Hash-Based Signatures
- Related work/possible work item
  - draft-hoffman-rfc6090bis-02: Fundamental Elliptic Curve Cryptography Algorithms
  - draft-mcgrew-hash-sigs-03: Hash-Based Signatures
- Expired
  - draft-irtf-cfrg-cipher-catalog-01: Ciphers in Use in the Internet

Work Item: Edwards-curve Digital Signature Algorithm (EdDSA)

- This was preferred by CFRG participants out of 5 proposals
- This continues to be a major work item for CFRG.

AOB