

CFRG Research Group

- Online Agenda and Slides at:
- <https://datatracker.ietf.org/meeting/96/agenda/cfrg/>
- Data tracker:
<http://datatracker.ietf.org/rg/cfrg/documents/>

Agenda

- <https://datatracker.ietf.org/meeting/96/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 Buenos Aires
- In RFC Editor's queue
 - None
- Completed, waiting for chairs
 - draft-irtf-cfrg-eddsa-05: Edwards-curve Digital Signature Algorithm (EdDSA) - **in IRSG review.**
 - draft-irtf-cfrg-pake-reqs-05: Requirements on PAKE schemes - **in IRSG review.**
- Active CFRG drafts
 - draft-irtf-cfrg-xmss-hash-based-signatures-06 (**updated**): XMSS: Extended Hash-Based Signatures - **RGLC completed, chairs to send to IRSG for review.**
 - draft-mcgrew-hash-sigs-04 (**updated**): Hash-Based Signatures.
 - draft-irtf-cfrg-argon2-00: The memory-hard Argon2 password hash and proof-of-work function
 - draft-irtf-gcmsiv-01: AES-GCM-SIV: nonce misuse-resistant authenticated encryption
 - draft-irtf-cfrg-spake2-03: SPAKE2, a PAKE
 - draft-irtf-cfrg-augpake-06 (**updated**): Augmented Password-Authenticated Key Exchange (AugPAKE)
- Related work/possible work item
 - 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 API

Crypto Review Panel

- Originally Suggested by Stephen Farrell (Sec AD)
- Proposal by CFRG Chairs, intended to supplement normal CFRG process with more structured reviews.
- May be used to review documents coming to CFRG, Security Area or Independent Stream.
- Expected workload: one/two reviews per year, produce short report with recommendations.
- Hiring now! Please send your nominations (and self-nominations) by September 9th 2016.

AOB