

DCRUP Working Group

IETF 99 – Prague, Czech Republic

Murray Kucherawy
Rich Salz
<dcrup-chairs@ietf.org>

Administrivia

Administrivia (chairs; 5 mins)

- Blue sheets, scribe, minute-taker
- Introduction
- Charter tweak

NOTE WELL

- Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:
 - The IETF plenary session
 - The IESG, or any member thereof on behalf of the IESG
 - Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
 - Any IETF working group or portion thereof
 - Any Birds of a Feather (BOF) session
 - The IAB or any member thereof on behalf of the IAB
 - The RFC Editor or the Internet-Drafts function
 - All IETF Contributions are subject to the rules of [RFC 5378](#) and [RFC 8179](#).
- Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.
- Please consult [RFC 5378](#) and [RFC 8179](#) for details.
- A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.
- A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

NOTE WELL, in other words

- You have the right to remain silent. Anything you say can be used by the IETF.
- You have the right to consult with an attorney with respect to your intellectual property rights and obligations prior to participating in any IETF context.

draft-ietf-dcrup-dkim-crypto

- John Levine, 15 minutes
 - To hash the key or not, that is the question. Well one of them, anyway.

draft-ietf-dcrup-dkim-usage

- Scott Kitterman, 5 minutes
 - Changing RSA key size
 - Moving to sha256
 - Still RSA PKCS1.5; do we need RSA-PSS?

draft-ietf-dcrup-dkim-ecc

- Scott Rose, 5 minutes
 - P256 ECDSA

Open Microphone / AOB

- (remaining time)