CURDLE at IETF-97

Rich Salz, co-chair

Agenda

- Administrivia: Note well, Scribe, Note-taker
- CMS Drafts
- DNSSec Drafts
- PKIX Drafts
- SSH Drafts
- The issue of “contexts”

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 3979 (updated by RFC 4879).
- 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 3979 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.

CMS Drafts

- draft-ietf-curdle-cms-chacha20-poly1305-03 – pub requested
- draft-ietf-curdle-cms-ecdh-new-curves *and* draft-ietf-curdle-cms-eddsa-signatures
  - Need a rev to align with PKIX draft, then ready for WGLC
  - We need reviewers and shepherd; anyone?

DNSSEC Draft

- draft-ietf-curdle-dnskey-eddsa-02 – in WGLC
  - Dcoument shepherd: Daniel

PKIX Drafts

- (Jim’s slides)
- Document shepherd: Daniel *(this does not scale)*

SSH Drafts

- draft-ietf-curdle-rsa-sha2
  - Ready for WGLC?
- And these three:
  - draft-ietf-curdle-ssh-ext-info (Extension Negotiation in Secure Shell (SSH))
  - draft-ietf-curdle-ssh-kex-sha2 (Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH))
  - draft-ietf-curdle-ssh-modp-dh-sha2 (More Modular Exponential (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH))
- Reviewers?

Contexts

- With no hat
  - We thought they were a good idea because TLS thought so
  - We've since learned we don't need them
- With co-chair hat
  - Suggest we say "use an empty context" whenever we use a signature format that has a context.
  - Discuss. Hum.
  - Any consensus will be confirmed on the list