DTLS/SRTP Protection Profiles for 256-bit AES-CTR Encryption

draft-lennox-avtcore-dtls-srtp-bigaes-00

Jonathan Lennox

AVTCORE, IETF 98

Overview

- draft-ietf-avt-dtls-srtp (RFC 5176) removed registrations for AES-256-based modes
  - because draft-ietf-avt-srtp-big-aes wasn't done
- But these registrations weren't then added to draft-ietf-avt-srtp-big-aes (RFC 6188)
- This draft registers them
  - Text is copied verbatim out of draft-ietf-avt-dtls-srtp-03
- These codepoints are actually already in libsrtp, since it implemented draft-ietf-avt-dtls-srtp before it was completed.

Why not just use GCM?

- RFC 7714 defines AES-256-GCM — why not just use that?
- You can — and should, if you can.
- But some implementations don't have GCM yet.
- We want to minimize difficulties of transitioning off SDesc, which has an AES256-CTR mode.

Thoughts?

- Does the group want to adopt this?
- Any objections?