SIP Security Overview

IETF 88 (Vancouver)

SIP Security and Usability

- Baseline SIP signaling
  - Digest auth, TLS, S/MIME for bodies (optional)
    - Decentralized, federated, beholden to CAs
  - But little adoption of TLS, less still of S/MIME
    - Deployability of certs to endpoints a major concern
- Media security
  - SRTP gives way DTLS/SRTP
  - Alternatives like zRTP in the marketplace (opportunistic)
- Connective tissue between signaling and media?
  - How to negotiate security keys for SRTP?
  - How to bind SIP-layer identities to media streams?
    - SIP Identity for URIs, ongoing work in STIR for telephone numbers
    - IdP work in RTCWeb