Topics

• Differences in -01
• Framework Outline Refresher
• Action Item List
Differences in -01

Simplify some entity names & reduced acronym dependence in text, diagrams.

• KMF >> Key Distributor
• MDD >> Media Distributor
Entities and Trust with Media

- **Endpoint**
  - Could also be a gateway, media transcoder/mixer other media-handling devices trusted by the enterprise

- **Key Distributor**

- **Call Processing**

- **Media Distributor**

- **Trusted Elements**

- **Untrusted w/ Media Content**
“Outer” (HBH) and “Inner” (E2E) Authenticated Encryption

Operational Details: draft-ietf-perc-double
E2E Keys

Generation

• An “Outer” SRTP master key is created by each endpoint, E2E Key(i), for media it transmits.

Confidentiality thereof

• A conference-wide key encryption key (ie, EKT Key) is used to encrypt an endpoint’s “Outer” master key for sharing with all the (valid) endpoints in a conference.

• Conference-wide key encryption key can change during the life of conference, such as triggered by an event.

• More Operational Details: draft-ietf-perc-srtp-ekt-diet
Where Keys Come From

• Key Distributor
  – Conference-wide key encryption key (EKT Key)
  – HBH Keys between Endpoints and Media Distributors (AX, BY)

• Endpoints, Media Distributors generate the others

More Operational Details: draft-jones-perc-dtls-tunnel
Framework Action Items

• Media Distributor requirements and constraints to rfc7667 topology mapping
  – TOPO-PtP-translator
  – SFM w/ single, common SSRC space
  – Others?

• Add a list of RTP header extensions that should/must not be E2E encrypted?
Framework Action Items (cont)

• Mapping of endpoints-to-a-given-conference may need to be conveyed.

• Possibly add ability for transmit-only (one-way) devices not trusted for two-way media (hence, would not receive any media from endpoints).

• Expand Entity Trust section
  – Certificate Fingerprint via signaling
  – Identity Assertions