Differences in -02

Administrative/Editorial end of spectrum:
• To Do List moved to https://github.com/ietf/perc-wg/issues
  – All were closed due to completion (subsequent slides) or addressed in one of the other WG I-Ds
• “Attacks on PERC” section renamed “Security Considerations”
Differences in -02 (cont.)

*Per action items from IETF 96 WG meeting:*

- MD added that it operates as SFM with the PERC systems constraints, including limits on what RTP headers cannot be altered
  - E.g., Single, common SSRC space option

- Removed To Do for investigation in to enabling one-way media injection (e.g., announcements)
  - No interest in room to pursue and likely modern conferences will use OOB means instead
Differences in -02 (cont.)

Per action items from IETF 96:

• Mapping of endpoints-to-a-given-conference may need to be conveyed.
  – Sect 5.3 summarizes, then points to Tunnel draft for operational details

• Added to Entity Trust section
  – Pointers to rtcweb-security-arch on identity assertions

• List of RTP header extensions that should/must not be E2E encrypted?
  – If ever listed, would appear in Double WG draft
PERC Framework Refresher

Back-up slides
Entities and Trust with Media

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

- **Key Distributor**

- **Call Processing**

- **Media Distributor**

**Trusted Elements**

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

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

Generation
• An “Outer” “Inner” 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” “Inner” 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](https://example.com/draft-jones-perc-dtls-tunnel)