Multi-Party Conferences with end-to-end Media Privacy

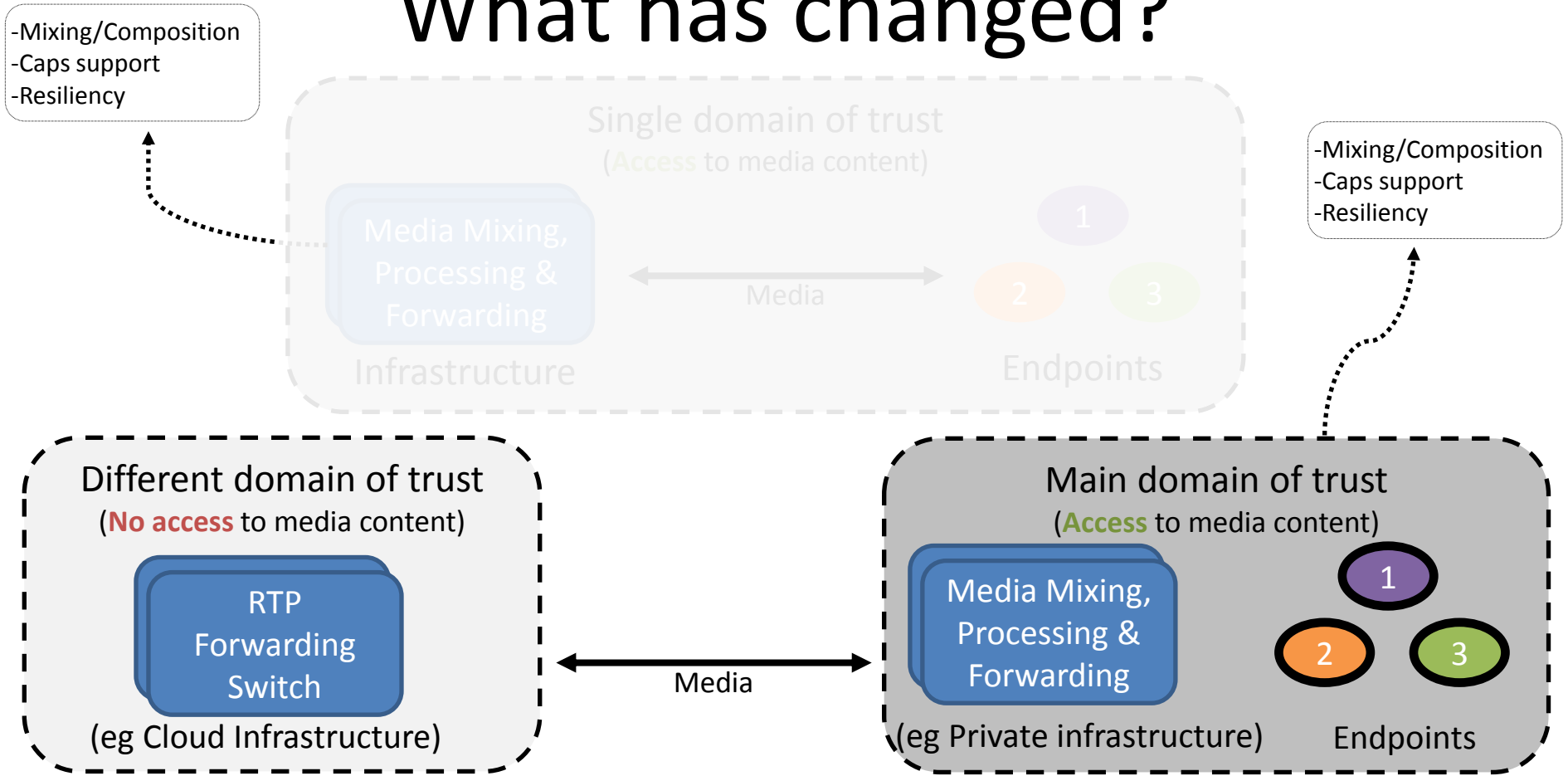
IETF 90 Toronto

AVT Core Working Group

Draft-ismail-avtcore-sec-media-req-00

Nermeen Ismail – Cisco Systems

What has changed?



RTP Forwarding Switch infrastructure must not access or modify media content without prior authorization

However

- Authorized RTP forwarding switch infrastructure needs to manipulate RTP header fields
  - RTP payload type
  - RTP extension headers
  - Potentially any field the SRTP encryption cipher is not dependent on
    - For current default cipher, SSRC & SeqNo can not be changed
- RTP forwarding switch infrastructure needs to forward streams to new receivers while current receivers exist

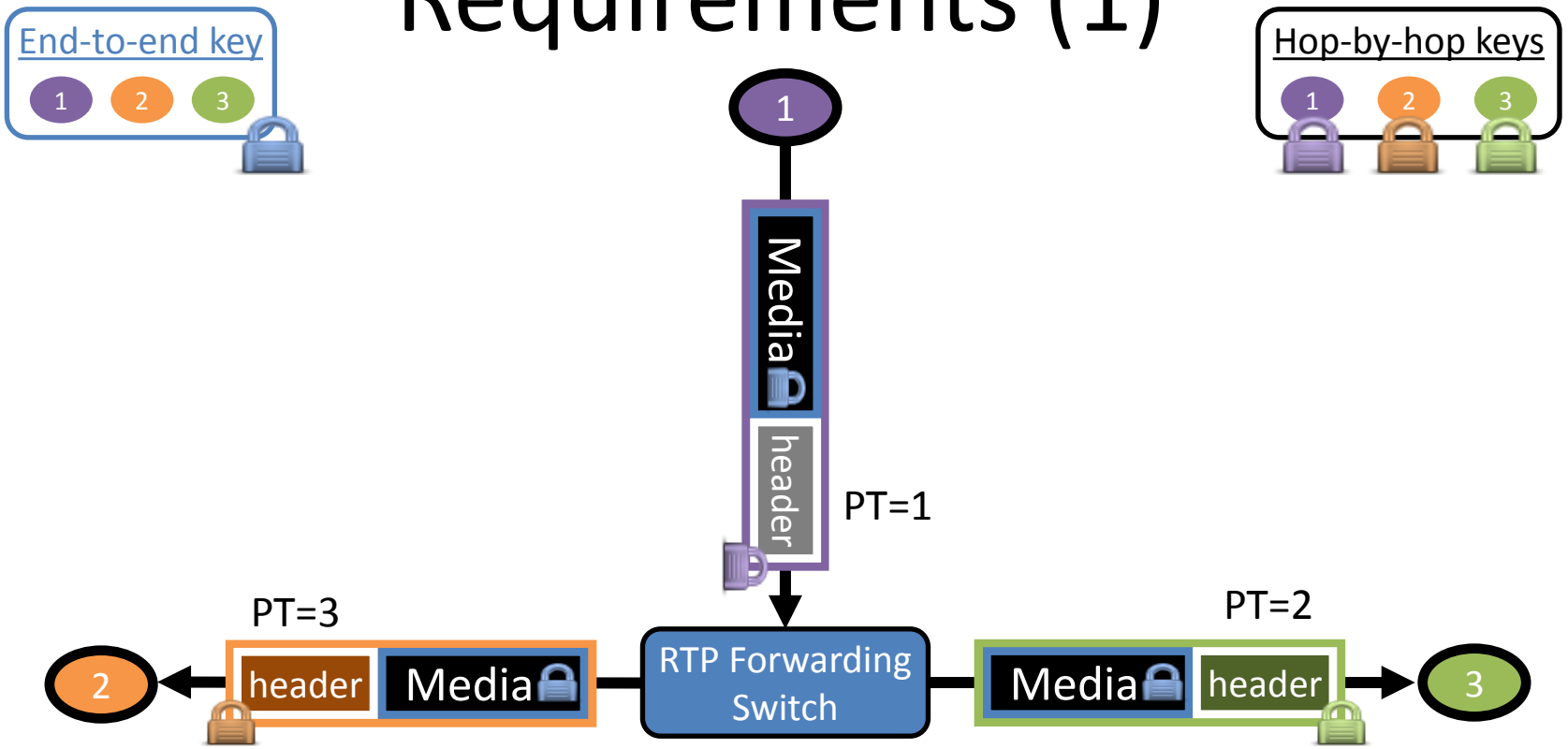
Requirements (1)

- RTP forwarding switch infrastructure must not generate, nor access, crypto keys used for media payload privacy and authentication without explicit authorization

- RTP forwarding switch can change any RTP header parameter, modulo SSRC and SeqNo/RoC for current default SRTP cipher

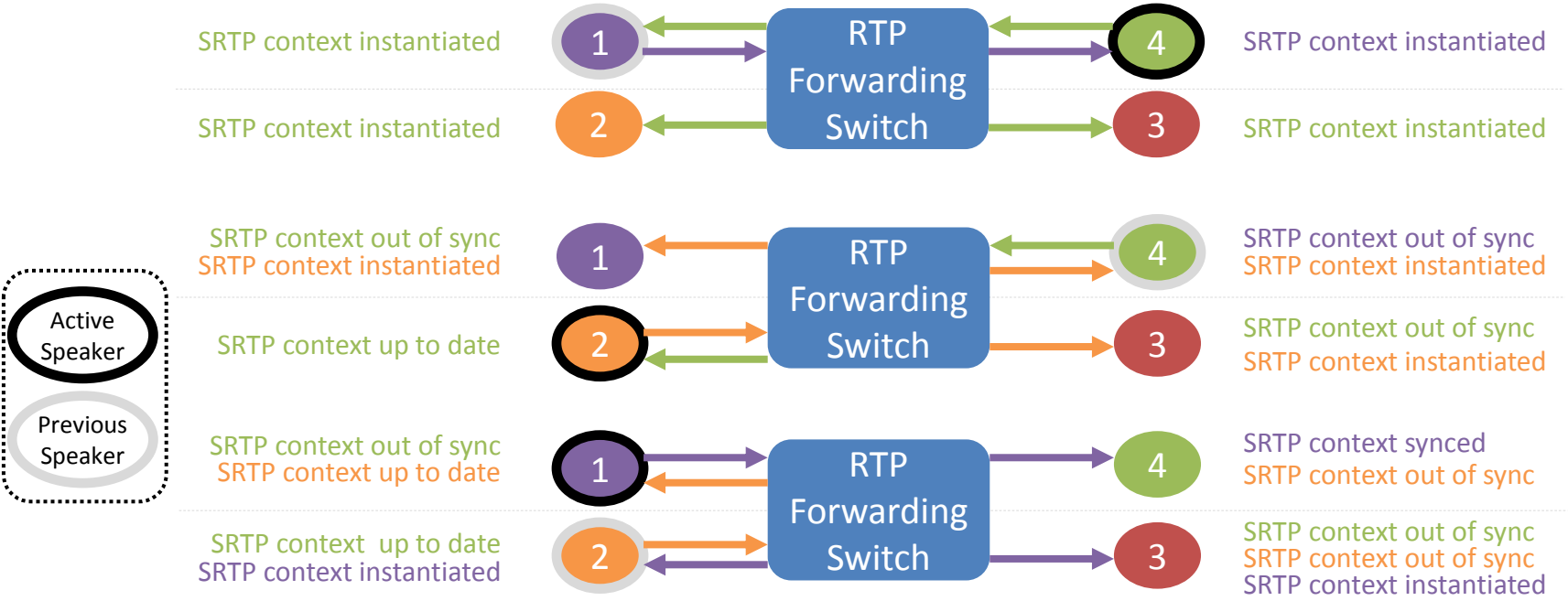
- Authentication and authorization for media privacy keys access must be independent of RTP forwarding switch infrastructure

Requirements (1)



Requirement (2)

- End to end SRTP context synchronization (RoC) between senders and changing set of receivers



Questions

- Enough interest to move forward with the work?
- Which WG for hardened use cases and requirements?
- Need a solution framework? Which WG?
  - RTP/SRTP
  - Key management (?)
  - Identity (?)