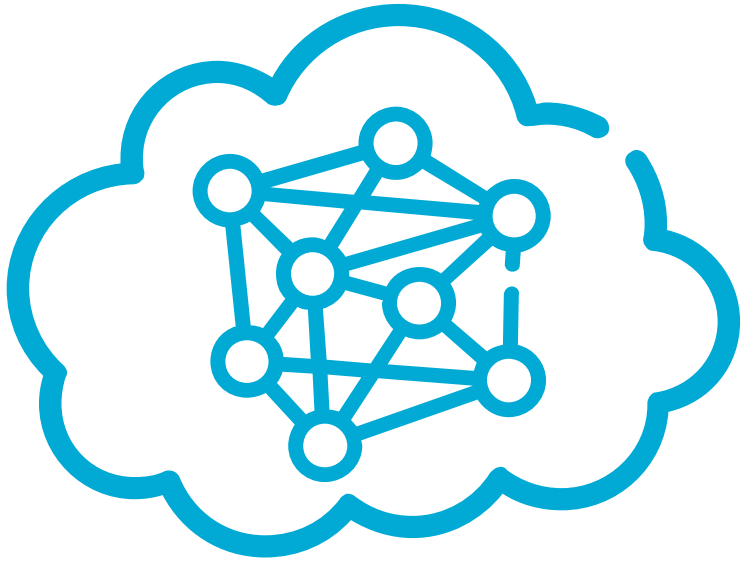
ERICSSON

SRTP FOR CLOUD SERVICES

DRAFT-MATTSSON-PERC-SRTP-CLOUD-00

JOHN MATTSSON
MATS NÄSLUND

MOTIVATION AND GOALS



- Update SRTP to support the transformation to cloud based, virtualized, and software based conferencing.

- This should be done in a way that:
  - Do not break RTP
  - Support relevant RTP topologies
  - Change SRTP and EKT as little as possible

SUPPORT RELEVANT RTP TOPOLOGIES

- Implicates that the media distribution device (MDD) shall be able to either:
  - Forward SSRC as is (SFM)
  - Change SSRC but keep a one-to-one mapping (SFM)
  - Change SSRC (Media Switching Mixer)

- MDD shall also be able to modify Payload Type (PT) and CSRC.

- Possible by making the SRTP transform independent of the RTP header.

DO NOT BREAK RTP

- Maintain consecutive sequence numbers
- Any switching will result in need to rewrite the sequence number.
- Rewrite sequence number instead of adding new metadata.
  - Avoid redefining existing mechanisms in RTP

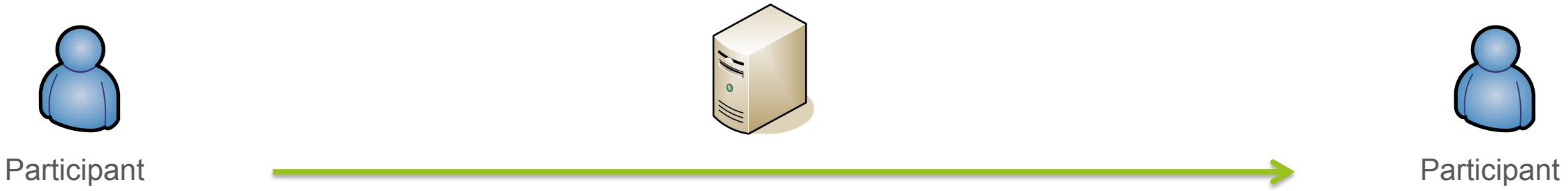
SMALL CHANGES TO SRTP AND EKT

- Supporting different RTP topologies means making the SRTP transform independent of the RTP header.

- Needed SRTP e2e functionality:
  - Context identification
  - Confidentiality
  - Message authentication
  - Replay

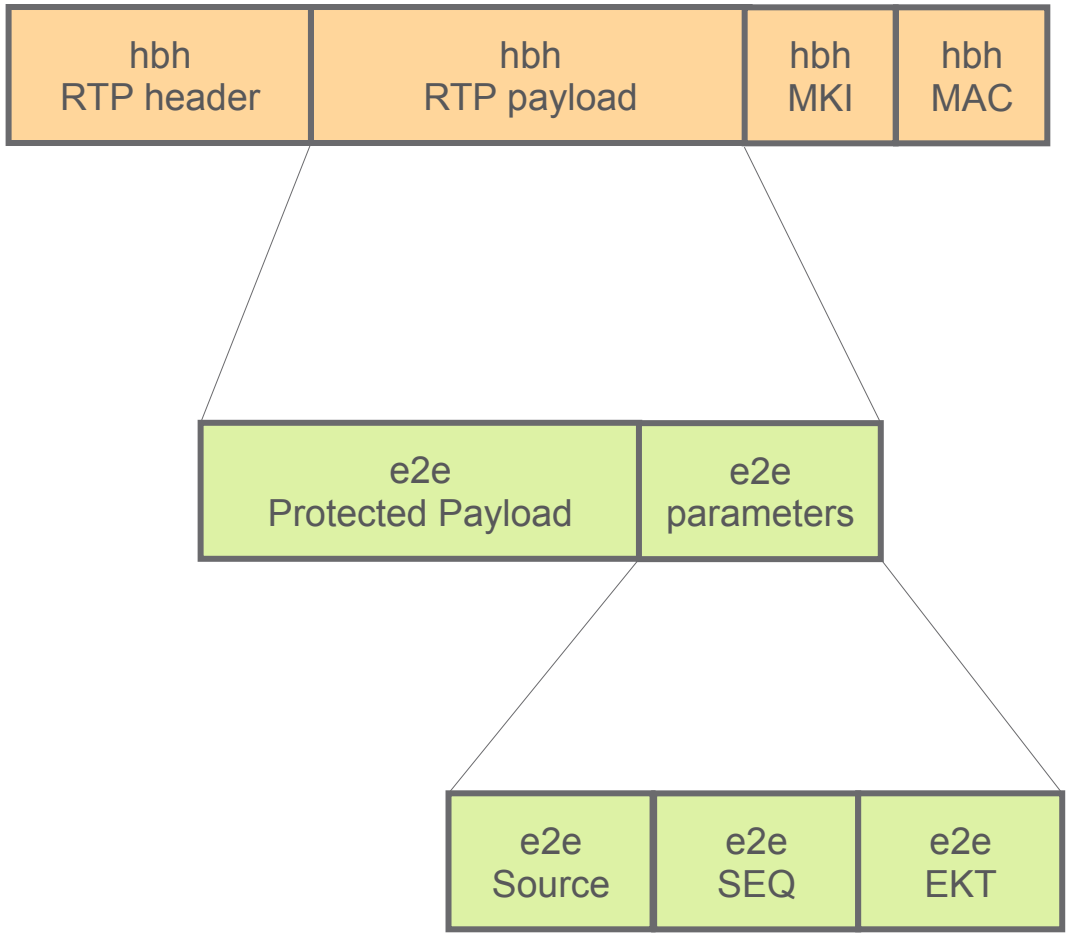
INFORMATION NEEDED E2E

- Three distinct information elements that needs to be communicated e2e.
  - ParticipantID: Identifier for the e2e participant.
  - StreamID: Identifier for a specific stream from a e2e participant.
  - PacketID: Identifier for a specific packet in that stream.



PACKET FORMAT

- No changes to RTP or the hbh part of SRTP.
- MDD forwards the payload as is.
- The hbh payload consists of an e2e protected payload (GCM) and e2e parameters.
- e2e parameters should include e2e source, e2e sequence, e2e EKT, etc.



DEFINE SRTP E2E TRANSFORM (GCM)

- Update SRTP Context identification

  <SSRC, IP, port> ➔ e2e parameters

- Update IV formation

  0x0000 II SSRC II SRTP Index ➔ IV = 0x0000 II e2e parameters

- Update associated data coverage

  Whole RTP Header ➔ Padding bit (P), Marker bit (M), e2e parameters

ERICSSON