EKT

DRAFT-IETF-AVTCORE-EKT-03

JOHN MATTSSON

INTRODUCTION

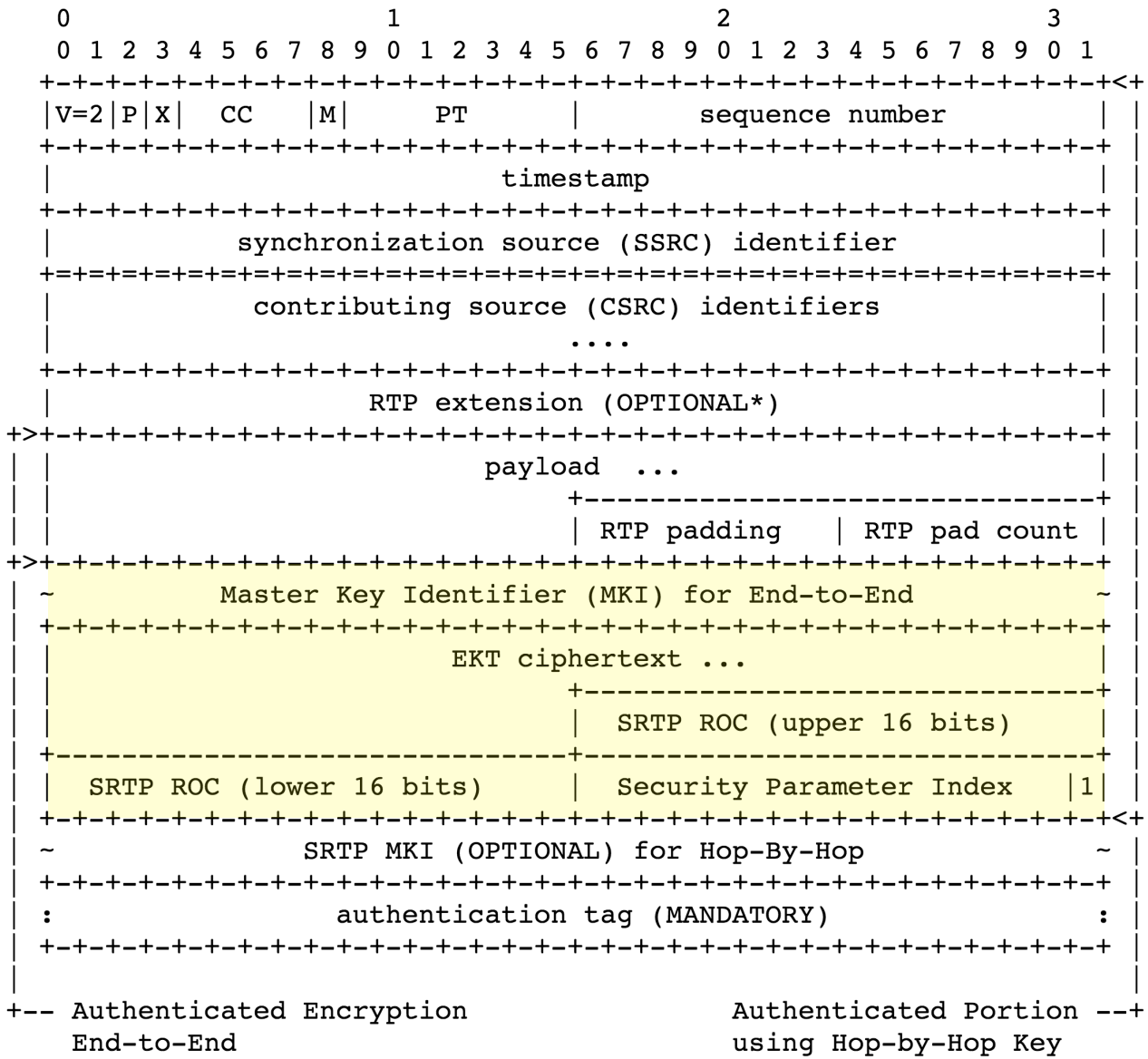
- No one has expressed a pressing need for EKT with its current feature set.
  - No need to standardize the current version of EKT.
- Currently agreement in PERC to use EKT for distributing the e2e SRTP Master Keys.
- Plan is to gather the requirements PERC will have on EKT and update the solution to meet these goals.
  - A single EKT document fulfilling also PERC's requirements.
- PERC has a lot of interest in, and ideas on how to update EKT.
  - But the PERC requirements for EKT is currently not clear or stable at the moment.
- Next version (-04) of EKT will not take PERC into account.

SUGGESTED CHANGES FOR -04

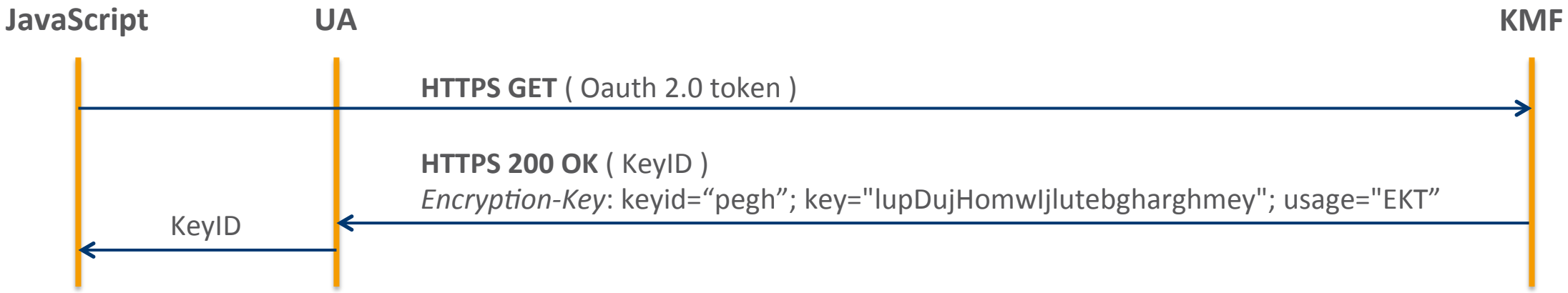
- Remove ISN (without replacing it with MKI).
  - ISN does not work with RTCP and has major problems with DoS.
  - A single SRTP Master Key per (EKT SPI, SSRC).
    - Rekeying SRTP Master Key requires new EKT Key
      - Receiver start using new SRTP Master Key upon receiving Full EKT Field.
- Require a single SRTP Master Key for SRTP and SRTCP
  - Free to send EKT in only RTP, only RTCP, or RTP and RTCP.
- EKT SPI negotiated by DTLS-SRTP and SDESC is 16 bits instead of 15
  - The MSb of the DTLS-SRTP and SDESC SPI parameter must be 0 (Paul Jones).
- EKT requires all endpoints to use the same SRTP transform / protection profile.
  - Introduce AEAD_AES_128_GCM as mandatory to implement for EKT.
- Some other clarifications on terminology and processing.

DRAFT-JONES-PERC-PRIVATE-MEDIA-FRAMEWORK

- A change to EKT such that the ROC is transmitted in the clear.
- A change to EKT to use MKI rather than ISN.
- A means through EKT or another mechanism to negotiate the SRTP security profiles for end-to-end.
- A means through EKT or another extension of sending the participant identifier.



DRAFT-WESTERLUND-PERC-WEBRTC-USE-CASE



- Distribute EKT Key in an HTTP Encryption-Key header (draft-thomson-http-encryption)
  - EKT Key stored by UA, JavaScript only gets KeyID

- When participant joins conference, derive New EKT Key = KDF(Old EKT Key)
  - Avoids having to distribute new EKT Key
  - Requires EKT key generation counter and SRTP MKI