DTLS-SRTP Key Transport ("KTR")

AVT Working Group

draft-wing-avt-dtls-srtp-key-transport-03

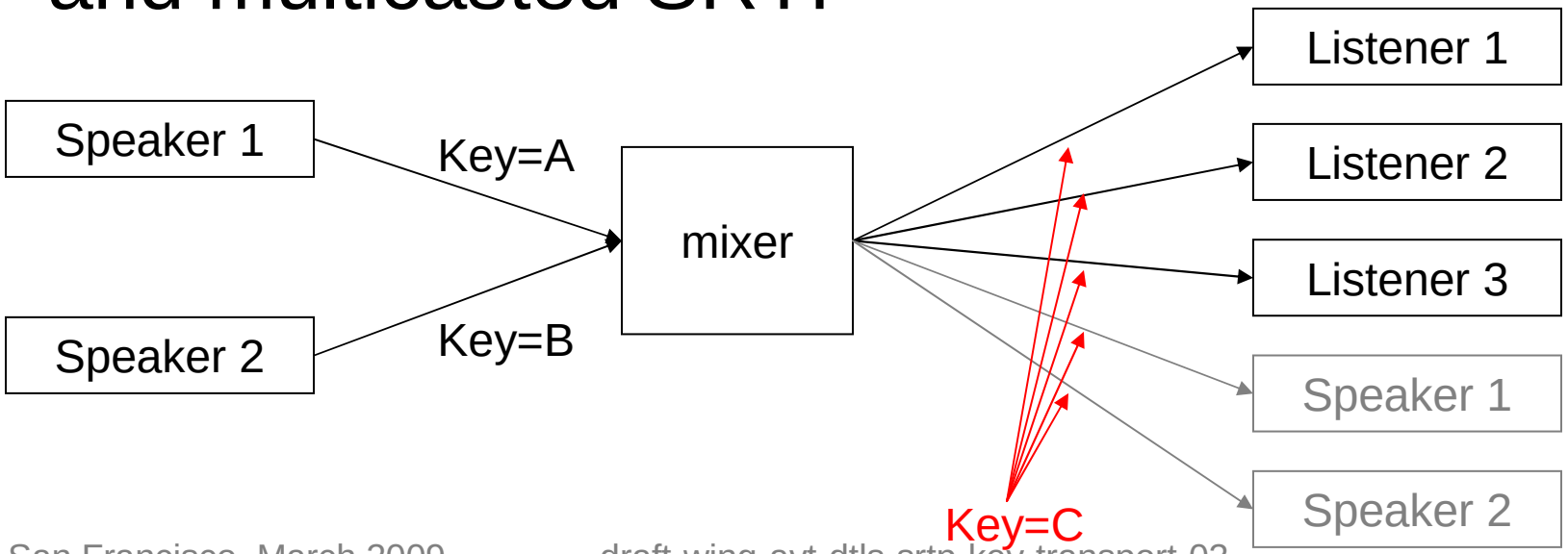
Dan Wing, dwing@cisco.com

Status

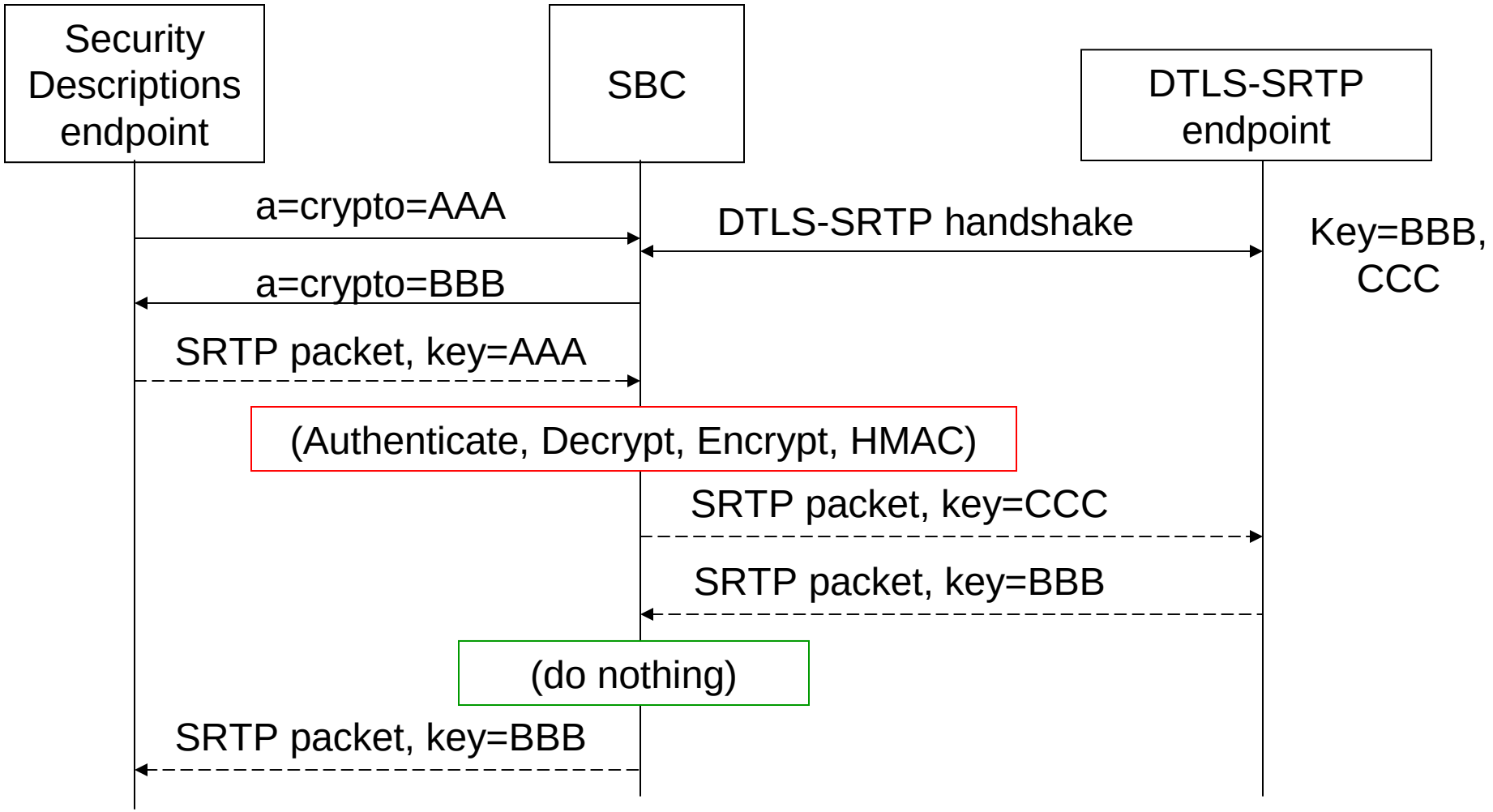
- Third presentation to AVT
- Changes since -02 (presented in Dublin)
  - Added EKT support
    - To transport EKT_KEY and related information
  - Removed Logical Key Hierarchy (LKH) per WG feedback

Key Transport Overview (1/3)

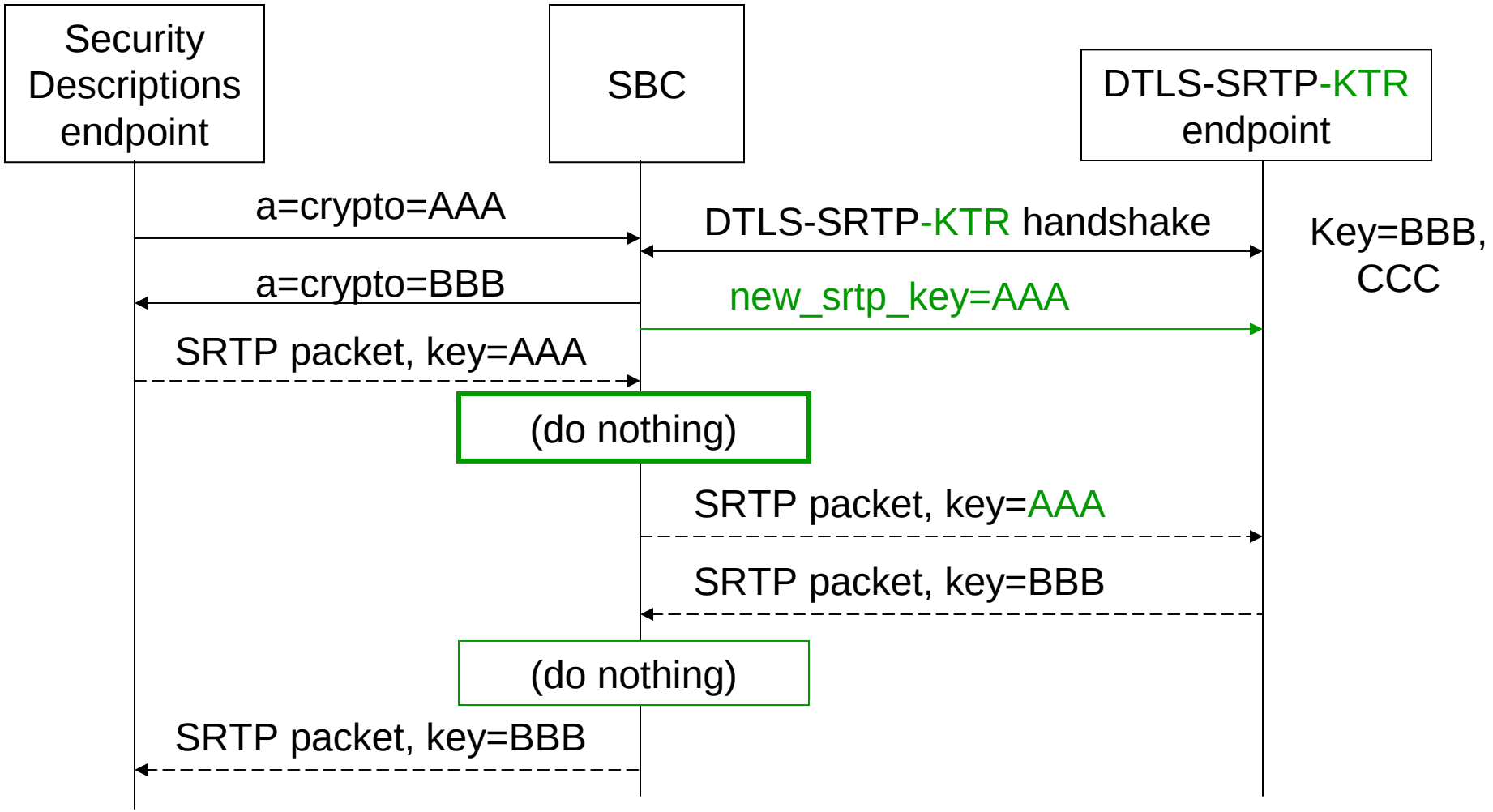
- Efficient SRTP operation for unicast audio or video conferencing
  - Avoids re-keying SRTP packets for each listener
- and multicasted SRTP



Without Key-Transport: CPU intensive in one direction (2/3)



With Key-Transport: CPU efficient (3/3)



Relationship to EKT

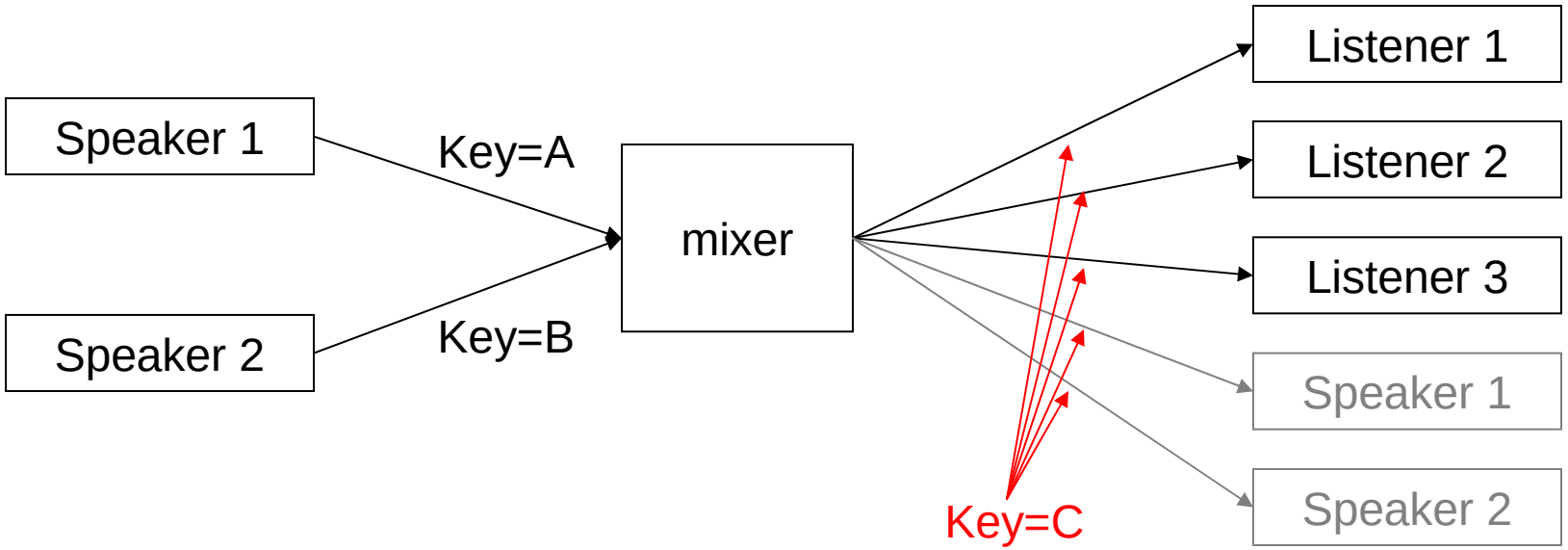
- DTLS-SRTP-Key-Transport can send EKT_Key (and related information)
- EKT can then perform SRTP re-keying
- EKT is even more efficient than DTLS-SRTP-Key-Transport for group keying
  - EKT are sent as RT(C)P packets
  - Arrive at same hosts running RT(C)P
- … But, EKT is additional engineering effort

draft-mcgrew-srtp-ekt-04

Backup Slides

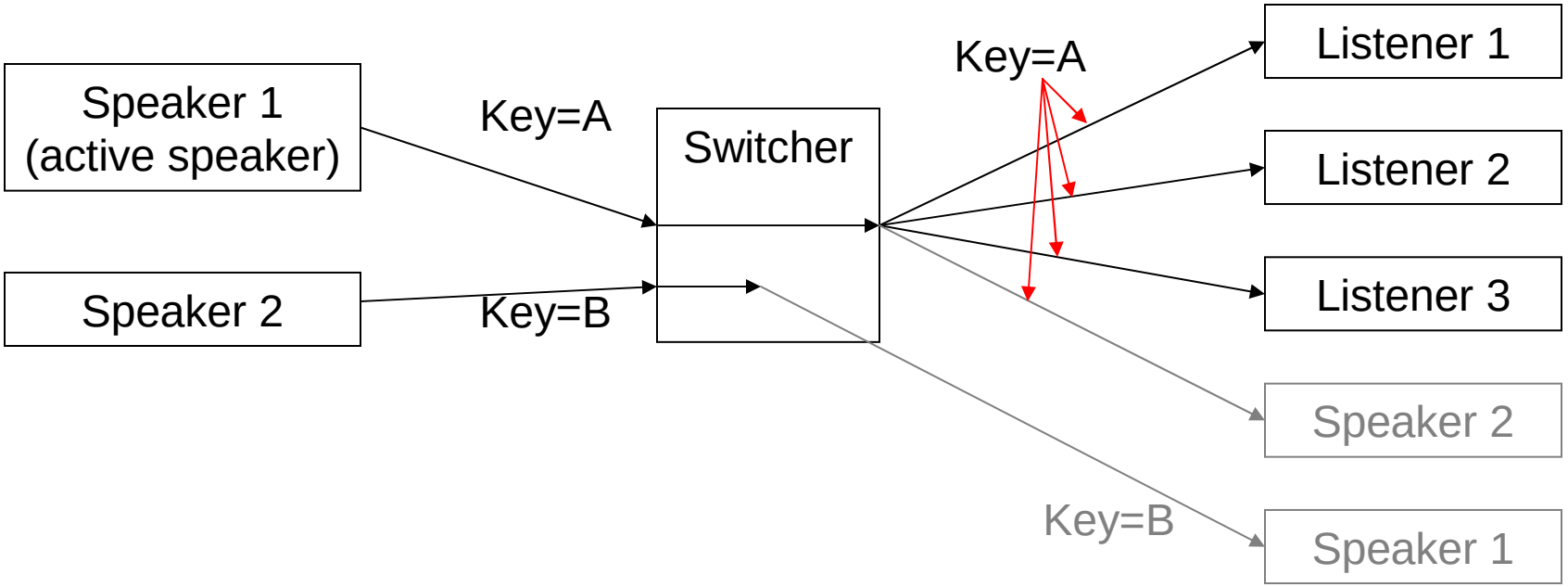
Point to Multipoint using RFC3550 Mixer Model

- Transport one SRTP key, inside of the per-listener DTLS session, to legitimate listeners



Point to Multipoint using Video Switching MCUs

- Transport speaker's keys to listeners
- SRTP packets not encrypted/decrypted by switcher



Point to Multipoint using Multicast

1. Each listener establishes unicast DTLS-SRTP session with speaker
2. Speaker uses DTLS-SRTP Key Transport to tell every listener the same SRTP key
3. (not shown) SRTP packets multicasted