# DTLS-SDP

IETF#95

Buenos Aires, Argentina

Christer Holmberg

Roman Shpount

# (2)

- Clarify the SDP Offer/Answer procedures for DTLS protected media
- Clarify when an SDP Offer/Answer transaction triggers a new DTLS association
  - Generic requirement to mandate new DTLS association on transport change (RFC 5763) removed.
- Define new SDP attribute to reference DTLS association
- Clarify usage of multiple fingerprints

# (3) SINCE YOKOHAMA

- WGLC
- ”dtls-connection” attribute replaced with ”dtls-association-id” attribute
  - WebRTC: possible to get multiple answers to an offer (not forking)
    - ’dtls-connection:new’ ambigous in such cases
  - Reference to DTLS association
  - Per direction
  - New reference value can be used to request new DTLS assocation if fingerprint and DTLS role does not change

# (4) NEW DTLS ASSOCIATION

A new DTLS association MUST be established in the following cases:

- The DTLS roles change
  - After O/A transaction is complete
    - Offer with ‘actpass’ does not change role
    - Answer may change role
- Fingerprint(s) change
  - Offer or Answer
- DTLS association ID changes
  - Offer or Answer

# (5) USE-CASES

- The following situations MAY require a new DTLS association
  - Change of Local Transport Parameters
  - Change of ICE ufrag value

- As the situations above do not always require change of DTLS role, or a new fingerprint value, the SDP “dtls-association-id” attribute is used to explicitly indicate whether a new DTLS association is required.

# (6) SDP ”dtls-association-id” attribute

- Reference to DTLS association
  - In case of non-muxed RTP and RTCP, reference to both DTLS associations
- New DTLS association may use previous reference value

# (7) Multiple fingerprints

- draft-holmberg-mmusic-4572-update
- Applies to both TLS and DTLS
- Use-cases:
  - Multiple certificates associated with single m- line
    - E.g. Separate certificates for RTP and RTCP (non-mux)
  - Multiple fingerprints for single certificate
    - Different hash functions
    - Incremental upgrade of network entities
      - Some entities support newer/better hash functions
    - Certificate must match with at least one fingerprint

# (8) NEXT STEPS

- Adopt draft-holmberg-mmusic-4572-update
- Submit new version of draft-ietf-mmusic-dtls-sdp
  - Implement additions/changes based on meeting discussions
  - Fix editoral issues
  - WGLC

# (9) THE END