DTLS-SDP
...not to be mistaken with SDP-DTLS

IETF#94
Yokohama, Japan
Christer Holmberg
Roman Shpount
• Clarify the SDP Offer/Answer procedures for DTLS protected media
• Clarify when an SDP Offer/Answer transaction triggers a new DTLS association
• Define new SDP attribute to explicitly indicate a new DTLS association
SINCE PRAGUE

• Draft was WG adopted
• Usage of ”connection” attribute replaced with new ”dtls-connection” attribute
• Clarification of offerless INVITE handling
NEW DTLS ASSOCIATION

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

- The DTLS roles change; or

- The fingerprint (certificate) value changes; or

- The establishment of a new DTLS association is explicitly signaled;

Generic requirement to mandate new DTLS association on transport change (RFC 5763) removed.

NOTE: The first two items list above are based on the procedures in RFC 5763. This draft adds the support for explicit signaling.
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-connection” attribute is used to explicitly indicate whether a new DTLS association is required.
SDP “dtls-connection” attribute

- Same as “connection” for TCP/TLS
- media-level
- Values:
  - new: Establish new DTLS association
  - existing: Keep existing DTLS association

- If you don’t like the name of the attribute, suggest a better one on the list...
Offerless INVITE

- When an endpoint receives a SIP INVITE request that does not contain an SDP offer, the endpoint must include an SDP offer in a reliable response to the request.

- **QUESTION**: What ‘dtls-connection’ attribute value to include?

- **SUGGESTION**: Include ‘dtls-connection:new’
  - Offerless INVITEs mostly used for call transfer, when a new DTLS association is needed
  - ‘dtls-connection:existing’ allowed, if there is a mechanism (not in scope of draft) to indicate it
UPDATE EXISTING DTLS USAGES

• Currently the following DTLS usages have been defined:
  – DTLS-SRTP (RFC 5763)
  – UDPTL-DTLS (RFC 7345)
  – SCTP-DTLS (draft-ietf-mmusic-sctp-sdp)
  – DTLS-SCTP (draft-ietf-mmusic-sctp-sdp)
  – BFCP-DTLS (draft-ietf-bfcpbis-rfc4582bis)

• **SUGGESTION:** Update those RFCs/drafts to reference/use draft-dtls-sdp
**NEXT STEPS**

- Submit new version of the draft
  - Implement additions/changes based on meeting discussions
  - Fix editorial issues
  - WGLC
THE END

THANKS FOR LISTENING!