Transporting the SDP attribute 'dtls-id' in TLS and DTLS

draft-jones-perc-dtls-id-00

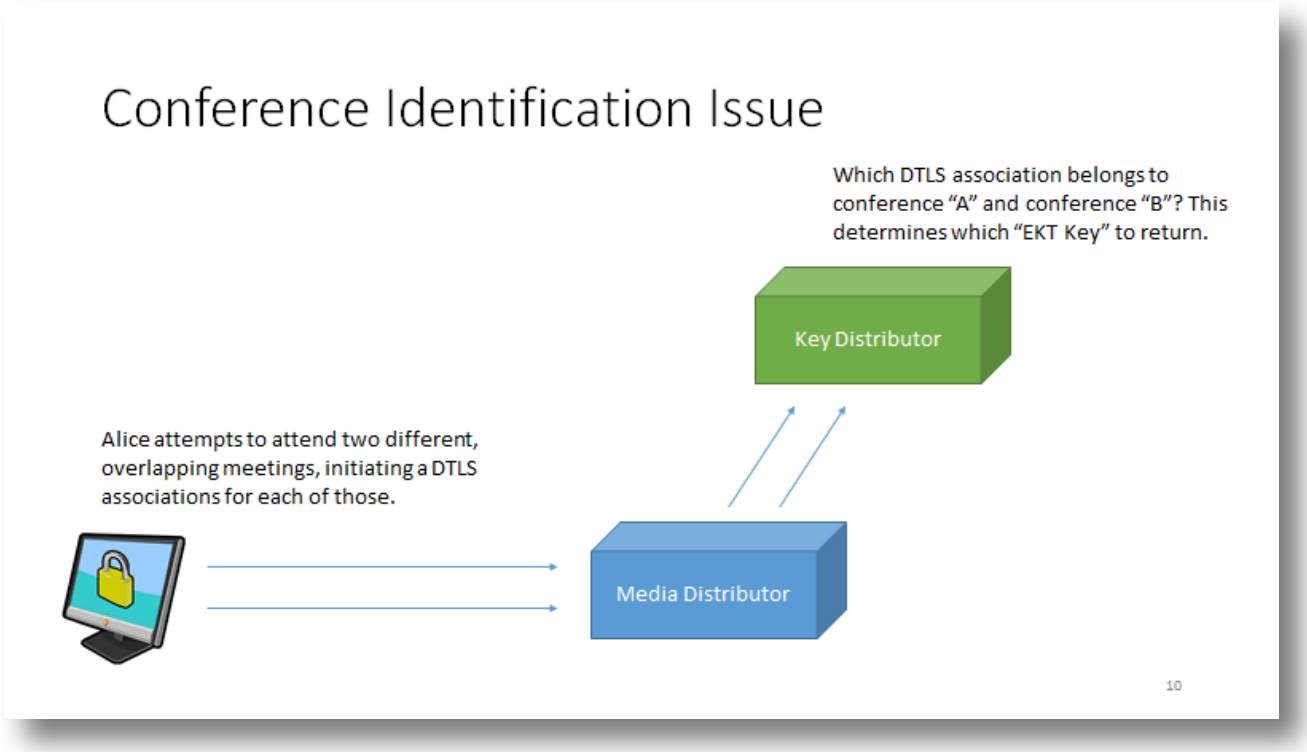
Paul E. Jones, Cisco

Nils H. Ohlmeier, Mozilla

IETF 98 • March 2017

Issue Considered

- The tunnel draft introduced a “conf_id” to address the “conference identification” issue raised previously
- It’s clunky
- It’s *another* conference ID
- No clarity on:
  - Which direction it is sent
    (MD ➔ KD or KD ➔ MD)
  - How it is associated with an incoming call



Proposal

- Given the “dtls-id”, which is unique per DTLS association, can be advertised in SDP and associated call control signaling [draft-ietf-mmusic-dtls-sdp], put that into the DTLS ClientOffer message as a DTLS extension
- It doesn’t need to be encrypted
  - Media Distributor could utilize this information if desired
- Get rid of the conf_id field in the DTLS tunnel draft
- We assume the Key Distributor somehow learns about Alice’s certificate fingerprints and associated dtls-id value
  - Knowledge of certificate fingerprints is an existing assumption

The ‘dtls-id’ Extension

- Defined as:

```
struct {
    opaque dtls_id<20..255>;
} SdpDtlsIdData;
```

Note: [draft-thomson-avtcore-sdp-uks-01], which was also produced for this meeting, defines the same extension, though allowing a length of 1..255.

Note: We do not propose defining this extension *within* the tunnel draft. We can reference draft-thomson-avtcore-sdp-uks now that it exists.

Expected Result using dtls-id

- Alice initiates two calls in parallel to join two separate conferences
- The certificate fingerprints and “dtls-id” attribute are delivered to the Key Distributor and associated with Alice
- When a DTLS association is established, the Key Distributor checks to ensure the dtls-id and certificate fingerprint are expected values and uses the dtls-id value to ensure the correct conference key is provided

Next Steps

- Move the procedural text into the Tunnel draft or framework
- Refer to draft-thomson-avtcore-sdp-uks from the tunnel draft