DTLS Tunnel between a Media Distributor and Key Distributor to Facilitate Key Exchange

draft-ietf-perc-dtls-tunnel-01

Paul E. Jones, Cisco
Paul M. Ellenbogen, Princeton
Nils H. Ohlmeier, Mozilla

IETF 99 • July 2017

What’s New

- Minor editorial changes
- Incorporated tls_id / tld-id
- Address comments raised during the last IETF meeting

tls_id

- The DTLS tunnel will now utilize the tls_id (formerly dtls_id)
- Endpoints are required to include tls-id in the SDP

Background:

- As discussed during the last IETF meeting, the tls_id will allow us to avoid going forward with a conference identifier. The issue was that Alice could initiate two calls at the same time for two different conferences and the key server would not otherwise be able to tell which DTLS association belongs wot which conference.

tls_id – Open Issue

- Regarding this text:

  The process through which the "tls-id" in SDP is conveyed to the key distributor is outside the scope of this document.

- We have this note:

  Editor's Note:

  - The above can be removed if we agree that the media distributor will always forward SDP to the key distributor.
  - That said, should the media server take on this function or should some other call control function do this?
  - The former assumes the media distributor always has the SDP.

- Editor’s Preference: Leave the text, delete the note

Tunneling Procedures

- Revised the text to (hopefully) make it clearer
- Removed DTLS-SRTP association / tunnel affinity requirement
- Explicitly state that mutual TLS authentication is required
- Require the key distributor to send EndpointDisconnect
  - Otherwise, the media distributor might not be aware of failed associations
- Association ID is now a UUID

Versioning

- Revised the text of the versioning procedures
- Introduce highest supported version field
- Version field only in first message

Protocol Syntax

- Changes were made to align with agreements at the last meeting
  - Shorter version length field / placement
  - Put the message type before message length
  - Versioning-related (noted on previous slide)

Example

- Binary encoding example updated to use the assigned codepoints for “double” ciphers