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

draft-ietf-perc-dtls-tunnel-00

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

IETF 98 • March 2017

What’s New

- Minor editorial changes
- Editor’s note on conference identifiers
- Changed the example ciphers in Section 7 to be “double” ciphers

Editor’s Note on Conference IDs

- We’ll cover in the dtls-id draft

Editor’s Note on Tunnel Affinity

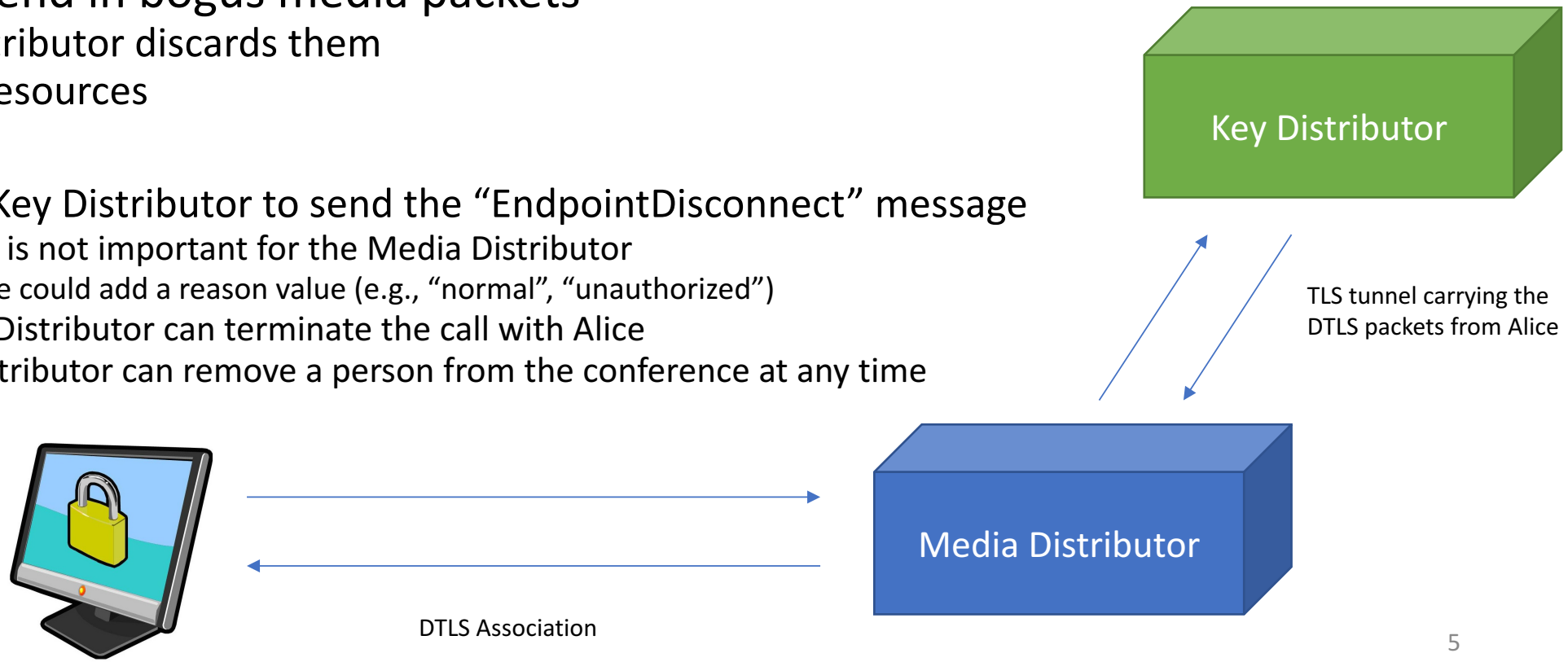
- Current Tunnel draft says this (and similar text for the key distributor):

  “The media distributor MUST forward all messages received from an endpoint for a given DTLS association through the same tunnel if more than one tunnel has been established between it and a key distributor.”

- Since connections break and multiple bi-directional TLS connections could exist, we propose:
  - Introduce a Media Server ID (a UUID) advertised in the first message from the Media Server to the Key Distributor when the tunnel is established
    - All messages should go to the same media server based on this UUID
  - If multiple key servers by the same name exists, we assume any one can receive messages for a given DTLS association

Enhancement to “EndpointDisconnected”

- Alice attempts to join a conference, but is not authorized
- Key Distributor rejects the association; Media Distributor unaware
- Alice could send in bogus media packets
  - Media Distributor discards them
  - Waste of resources
- Proposal:
  - Allow the Key Distributor to send the “EndpointDisconnect” message
    - Reason is not important for the Media Distributor
      - We could add a reason value (e.g., “normal”, “unauthorized”)
    - Media Distributor can terminate the call with Alice
    - Key Distributor can remove a person from the conference at any time



Other Suggestions Received

- Put the version field only in the first message sent
- Use a UUID (or otherwise long random value) for the association ID
- Have a message length before msg_type
- “highest supported version” in the UnsupportedVersion message