MDD/KMF DTLS Tunnel
A Proposal for Enabling Endpoint / KMF Key Exchange

Paul E. Jones
IETF #95 • Buenos Aires
April 4, 2016
Tunnel Objectives

- No changes to DTLS, DTLS-SRTP, etc.
- MDD and KMF establish a DTLS association (the “tunnel”)
- Endpoint and KMF establish a DTLS association
  - MDD forwards DTLS packets over the tunnel
  - KMF sends DTLS packets over the same tunnel
- Reliability is left to DTLS (no new mechanics or requirements)
- KMF also gives the MDD the HBH keys, salt values, and cipher for SRTP between MDD and endpoint
The Tunnel

- The MDD establishes a DTLS association with KMF
Tunneling DTLS from Alice

- Alice establishes a DTLS association with the KMF by sending DTLS packets toward the MDD
- MDD forwards Alice’s DTLS packets to the KMF via the tunnel as application data
  - MDD assigns an association identifier for the DTLS association (facilitates forwarding responses back to Alice)
  - MDD indicates supported security profiles for HBH operations via the tunnel
Tunneling DTLS from the KMF

- KMF sends DTLS messages back to Alice via the tunnel
- MDD forwards tunneled message on to Alice
  - Tunneling protocol includes association identifier previously assigned by the MDD, facilitating correct forwarding to Alice
  - KMF shares the HBH keys, salt values & cipher with the MDD when it sends the FINISHED message to Alice
Message Exchange via the Tunnel

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>MDD</th>
<th>KMF</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="#">Diagram showing DTLS handshake message exchange</a></td>
<td>Tunnel + Profiles</td>
<td></td>
</tr>
<tr>
<td><a href="#">Diagram showing DTLS handshake message exchange</a></td>
<td>Tunnel + Profiles</td>
<td></td>
</tr>
<tr>
<td><a href="#">Diagram showing DTLS handshake message exchange</a></td>
<td>Tunnel + Key Info</td>
<td></td>
</tr>
</tbody>
</table>

*.... may be multiple handshake messages ...*

---

*(Diagram showing DTLS handshake message exchange)*

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>MDD</th>
<th>KMF</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DTLS handshake message</td>
<td>Tunnel + Profiles</td>
<td></td>
</tr>
<tr>
<td>DTLS handshake message</td>
<td>Tunnel + Profiles</td>
<td></td>
</tr>
<tr>
<td>DTLS handshake message (including Finished)</td>
<td>Tunnel + Key Info</td>
<td></td>
</tr>
</tbody>
</table>

---

*(Diagram showing DTLS handshake message exchange)*
Tunnel Message Format

0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------+---------------+-------------------------------+
| Version (H)   | Version (L)   |                               |
+---------------+---------------+                               |
|                                                               |
|   Association Identifier                                      |
|                                                               |
|                               +-------------------------------+           |
|                               | DTLS Message Length          |           |
+-------------------------------+-------------------------------+           |
:                                                               :
:                     Tunneled DTLS Message                     :
:                                                               :
Messages from MDD to KMF
Messages from KMF to MDD (1)

This is just the “tunnel” message with no additional data appended
The message form when the KMF sends a FINISHED message to an endpoint. The extra data are the key, salt, and cipher values the MDD will use for HBH operations.