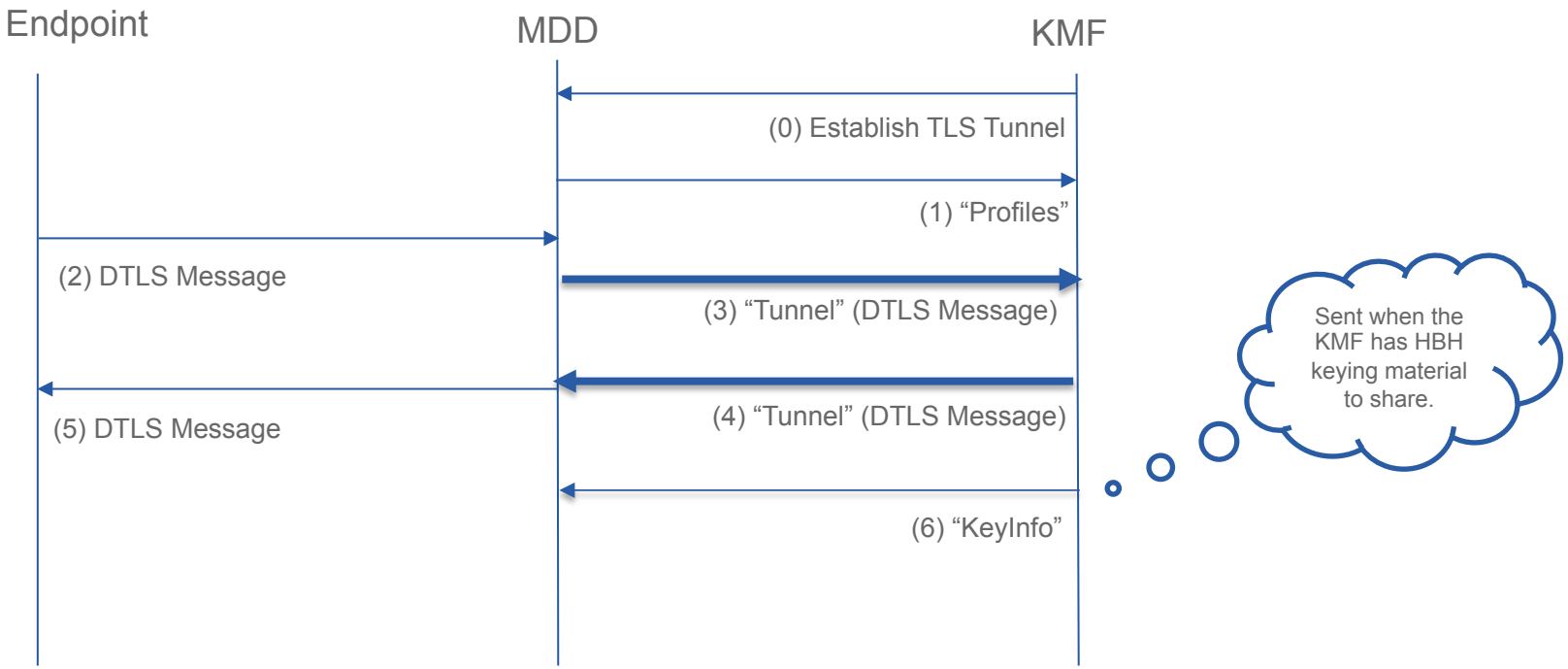
Proposed Tunnel Protocol

A move from DTLS to TLS

Paul E. Jones
PERC Interim
27 April 2016

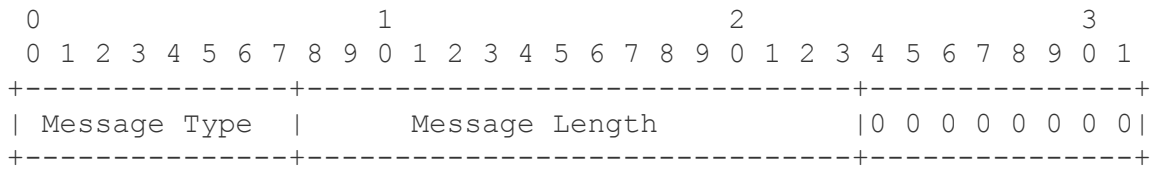
Sample Message Flow



Message Table

ID	Message
0x01	“Profiles” message
0x02	“KeyInfo” message
0x03	“Tunnel” message intended to carry tunneled DTLS packets

Common Message Header

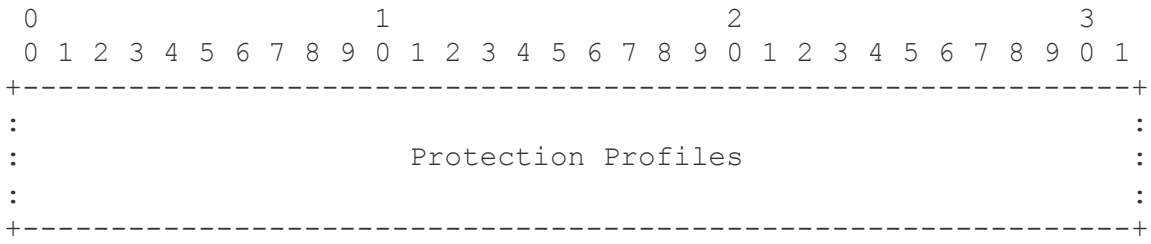


Message type: the type of message that follows.

Message length: the length of the entire message in octets, excluding the common header.

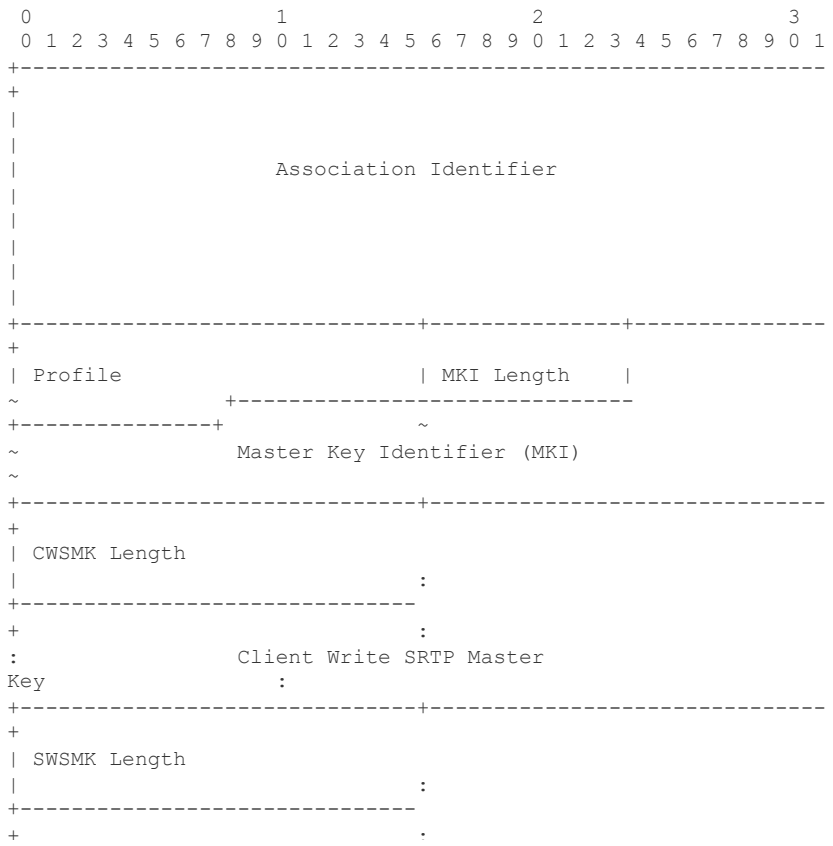
For all messages, the message body (if any) follows the common header.

“Profiles” Message (Message Type = 1)



Protection Profiles: This is an array of two-octet SRTP protection profile values as per [@!RFC5764], with each value represented in network byte order.

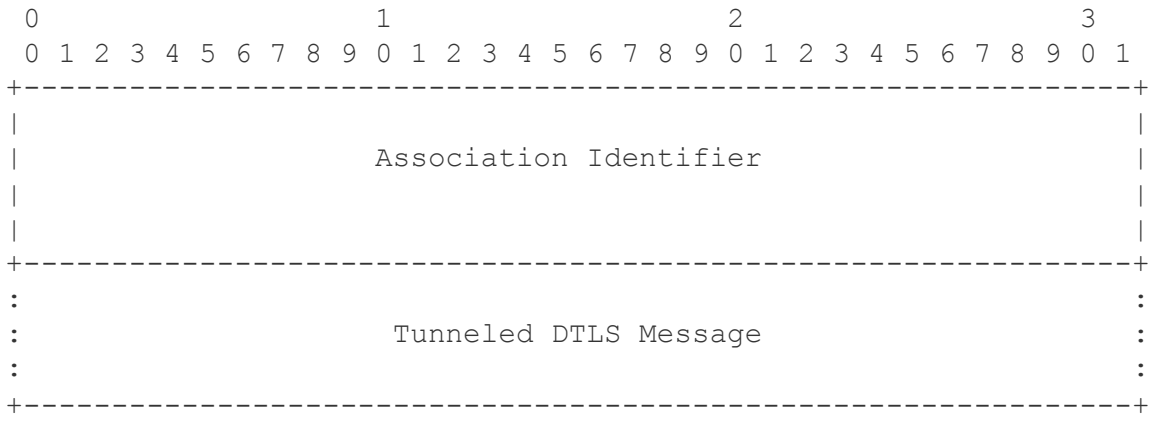
“KeyInfo” Message (Message Type = 2)



Association Identifier: This is the 16-octet(*) association identifier allocated by the MDD for each distinct DTLS association to which this message relates.

Profile: The SRTP protection profile (see [@!RFC5764]) the MDD MUST for HBH operations.

“Tunnel” Message (Message Type = 3)



Association Identifier: This is the 16-octet(*) association identifier allocated by the MDD for each distinct DTLS association that will be established.

Tunneled DTLS Message: This is the DTLS message exchanged between the endpoint and KMF.


CISCO