PERC Virtual Interim

27 April 2016

WG Roadmap

Signaling
Key management ← you are here
SRTP/SRTCP transforms ← (documents adopted now)

Today:

Requirements / architecture discussion for KMF-MDD protocol

PERC is creating an entity with intermediate privilege

Normal SRTP/SRTCP divides the world into two classes:

- In the session: Can encrypt / decrypt payload, MAC/verify headers + payload
- Not in the session: Can observe header fields, encrypted payload

PERC is about creating an entity **intermediate** between these two

- Not in the session, but gets some capabilities that things in the session have
- MDD = Network Attacker + (minimum privilege to do conferencing)

PERC key management assigns these roles

Basic requirement: Establish and distribute two crypto contexts

1. HbH context shared among participants AND MDD
2. E2E context shared among participants AND NOT MDD

E2E and HbH contexts => normal SRTP participant, full access

only HbH context => intermediate participant, partial access (i.e., the MDD)

What does the KMF do?

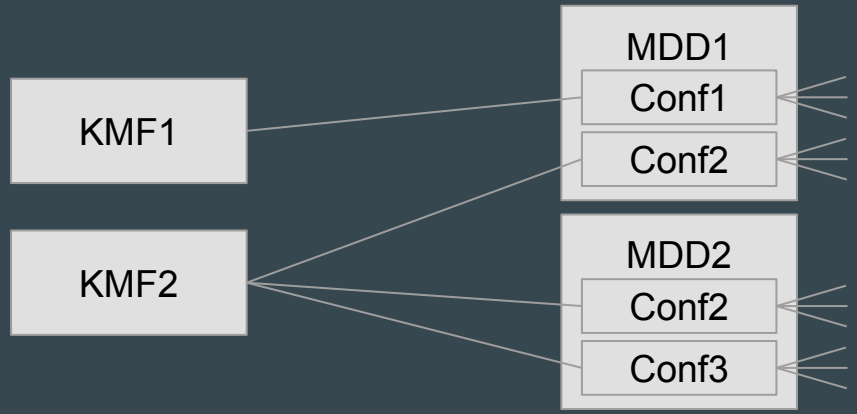
- Distributes E2E and HbH contexts to participants
- **Distributes the HbH context to the MDD** ← **need a protocol for this**
- Authenticates to participants (at the DTLS layer)
- Participants authenticate to it (also DTLS)
- [[Might be further identity / authentication]]

Topic today: A protocol for KMF-MDD interactions

Requirements for the KMF-MDD Protocol

Assumptions

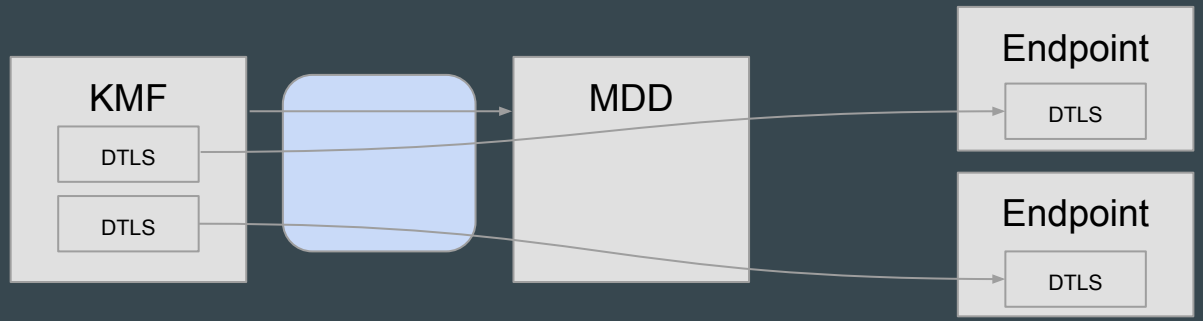
1. KMF-MDD relationship is configured out of band
   - e.g., which KMF is responsible for each conference
2. One KMF-MDD protocol session per conference on the MDD
   - No need to multiplex multiple conferences on a single KMF-MDD protocol session
   - KMF might have multiple tunnels to different MDDs serving the same conference



Functional Requirements

The KMF-MDD protocol must enable:

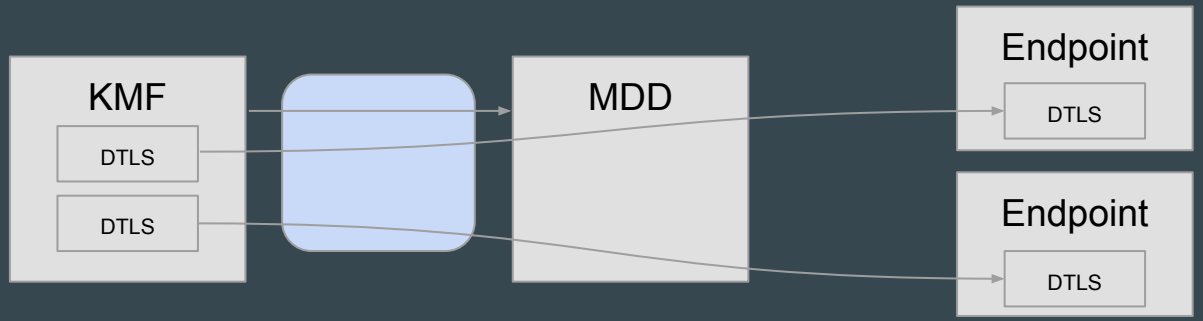
1. MDD to tell the KMF its supported protection profiles for HBH operations
2. KMF to tell the MDD the HBH cipher, key & salts
3. Bi-directional exchange of DTLS packets between end-points & the KMF via the MDD



Transport Requirements

The KMF-MDD protocol must:

- Reliably convey KMF-MDD information (profiles, keys, salts)
- Provide unreliable transport for DTLS packets
- Use secure, mutually authenticated transport for KMF-MDD information
- May use secure transport for DTLS packets
- Enable the MDD to demultiplex DTLS packets received from the KMF to the correct endpoints



… over to Paul …

Thank You