TLS/DTLS PSK Identity Extension

Jayaraghavendran K/Raja Ashok
Huawei Technologies
Problem / Motivation

- Existing PSK based handshake
  - Takes 2 RTTs
  - Handshake failure due to PSK ID mismatch is identified at 5th message (2nd RTT).

- Expected Improvements
  - Reduction in RTT
  - Reduction in number of handshake messages
  - Early PSK ID Mismatch Detection / PSK ID Negotiation.

- TLS 1.3 already solves this problem. But, DTLS 1.2 is heading for heavy deployment in IoT devices. DTLS 1.3 will take time for adoption.

- A Solution for DTLS 1.2 along the lines of TLS 1.3 will be very helpful
Proposed Solution

- New Extension for PSK Identity Negotiation
- Client to send it’s PSK Identities in it’s Client Hello
- Server uses this information in it’s Cipher Selection Process
- If PSK based Cipher is chosen, then Server includes this extension with selected PSK Identity in the Server Hello
- Server then directly proceeds to ChangeCipherSpec and Finished Messages (Resumption Flow)
- If none of the PSK Identities received from Client are present in Server, then Server either chooses a different cipher or aborts the handshake
DTLS/TLS PSK Abbreviated Handshake

1. Client Hello \textbf{(Carries PSK Identity as Extension)}
2. Server Hello \textbf{(Carries selected PSK Identity as Extension)}
   - (3) Change Cipher Spec,
   - (4) Finished
   - Application Data
3. Change Cipher Spec,
4. Finished
5. Application Data

opaque psk_identity<1..2^{16}-1>;

struct{
    select (Role){
        case client:
            psk_identity identity_list<1..2^{16}-1>;
        case server:
            psk_identity identity;
    }
}PSKIdentityExtension;
Thank You : )