An additional mode of key distribution in MIKEY draft-ietf-msec-mikey-rsa-r

D. Ignjatic, L. Dondeti,

F. Audet, P. Lin

Status

- draft-ignjatic-msec-mikey-rsa-r presented at IETF 62nd meeting
- draft-ietf-msec-mikey-rsa-r WG work item
- Added better support for multicast (by the inclusion of the GenExt(CSBID) payload
- WGLC some time in Nov 05.
  - expected to be met

Summary of Changes

- GenExt(CSBID) added to let the Responder generate all keying material
- ID|CERT payloads optional for cases where ID may be extracted from transport protocol (SIP)
- DoS prevention capabilities clearly spelled out in Security Considerations section

Summary of Changes

- If the Initiator does not specify a policy (does not include SP payload), the Responder MUST include it
- Responder MUST send an Error message "Message type not supported" (Error no. 13), if it cannot correctly parse the received MIKEY message – added to the table in 6.12 of RFC3830

Outstanding Issues

- Multiple media lines support with a session level MIKEY line
  - Single TGK multiple media streams
  - Absolute position of a stream in SRTP-ID map affects key derivation
  - If different Initiators offer different number of streams the Responder needs to be able to correctly map the keys to streams