MIKEY

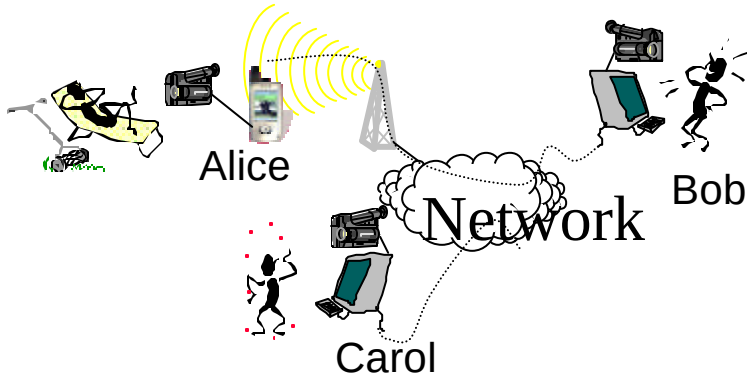
update

elisabetta.carrara@era.ericsson.se

Status

- MIKEY finished the WG Last Call, end of September.
- It has undergone no major changes.
- MIKEY implementation exists (works with SRTP).

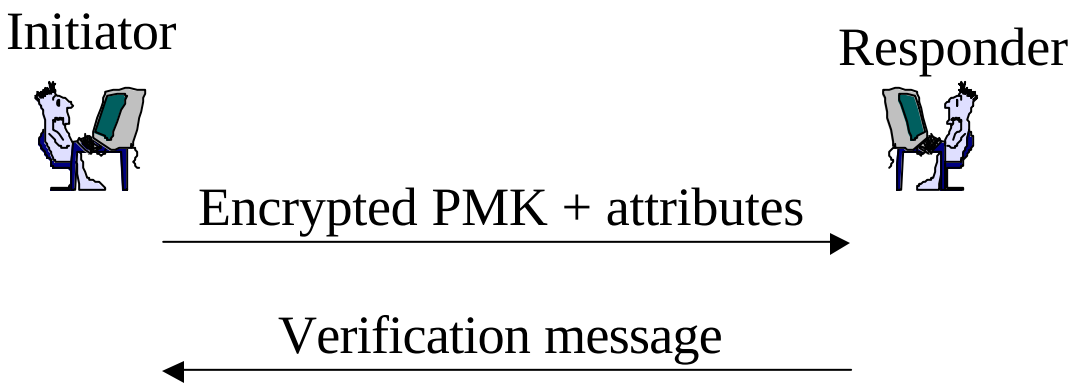
Overview



- Key management protocol to support multimedia security protocols, e.g. SRTP
- Possibility to have one negotiation for multiple “crypto sessions” (e.g. negotiate the security for both one SRTP audio session and one SRTP video session)
- Possibility to run over SIP and RTSP

Key transport and exchange mechanisms

- Pre-shared key based
- Public key based
- Diffie-Hellman based



Example: Key transport

<draft-ietf-msec-mikey-**04**.txt> (August)

- Added text explaining which keys are derived via the PRF function
- Payloads are byte-aligned
- Clarification: certificate and identity payload are different payloads

<draft-ietf-msec-mikey-**05**.txt> (October)

- IANA Consideration update (added text to request port)
- Change of notation in the Policy payload definition

- Editorial updates...