MIKEY-ECC

Andy Milne
Mitch Blaser
Dan Brown

Lakshminath Dondeti

MIKEY-ECC

- Proposes three modes
  - MIKEY-ECIES
    - ½ an RTT
  - MIKEY-DHSIGN with EC groups
    - Does this address Steffen's question?
    - Full RTT?
  - MIKEY-MQV
    - ½ an RTT

ECIES doesn’t use envelope keys

- ECIES: HDR, T, RAND, [IDi|CERTi], [IDr], {SP}, ECCPT, KEMAC, [CHASH], SIGNi
  - The ephemeral public key transmitted by the initiator, is transmitted in an ECCPT payload (see section 5.1) preceding the KEMAC payload.
  - The ciphertext and message digest required under ECIES are transmitted in the KEMAC payload, as in other forms of the MIKEY protocol.
  - The encryption key and HMAC key in use in the KEMAC are those extracted from the shared key derived using ECIES.
  - The PKE payload is not used.
- MRSA: HDR, T, RAND, [IDi|CERTi], [IDr], {SP}, KEMAC, [CHASH], PKE, SIGNi

What next

- Dec 2005 is the deadline for this
- Are folks comfortable with this?
  - If not, we need detailed reviews on why