

MIKEY: Multimedia Internet KEYing

(draft-ietf-msec-mikey-07.txt)

Fredrik Lindholm

Current Status

- AD Evaluation (by Russ)
- Main discussions
 - DH mode
 - Authorization discussions

Updates

- A new section added for discussion about authorization
- The DH mode is now OPTIONAL
- Description of how to add a new DH group added

Updates (cont.)

- AES Key Wrap added as an optional mode for key encryption
- New field in signature payload (to signal the signature algorithm used)

Comments?

Questions?