# HMAC-authenticated Diffie-Hellman for MIKEY

**IETF #57 Vienna 2003**

Dipl.-Inform. Martin Euchner
Siemens AG, Information & Communication Networks, M SR 3
81359 Munich, Germany
Tel: +49 89 722 55790 E-mail: martin.euchner@siemens.com

**draft-ietf-msec-mikey-dhhmac-02.txt**

**Update**

# Changes against –01.txt

- Only editorial changes and clarifications.
- Alignment with MIKEY-07 was not yet possible (too late!)
- Section 1: Relationship with MIKEY pointed out.
- Sections 1.1 and 5.3: Optional [X], [X, Y] defined and clarified.
- Sections 3 and 5.2: ID payloads clarified:
  - Initiator SHOULD include IDi payload,
    responder SHALL include IDi and SHOULD include IDr.
  - Identity information may be supplied by surrounding protocol.
  - Warning stated, that omitting ID information may weaken security.

# More changes against –01.txt

- Section 3.1: Combination of options defined in key update procedure:
  - a) key update: initiator and responder SHALL provide new, fresh DH payloads.
  - b) non-key related update (e.g. security policy update): [DHi] and [DHr, DHi] SHALL be left out.

- Section 5.2: Bidding-down attacks with multiple offered KM protocols addressed:
  - All key management protocol identifiers must be listed within the MIKEY General Extension Payload.
  - The General Extension Payload must be integrity-protected with the HMAC using the shared secret.
  - The protocol identifier for DHHMAC shall be "mikeydhhmac”.

# Yet more changes against –01.txt

- Section 5.3: Relationship with MIKEY explained: roundtrip, performance.
- Sections 5.3, 5.5:
  - More text due to DH resolution discussion incorporated;
  - addressing PFS, security robustness of DH,
  - generalization capability of DH to general groups in particular EC and “future-proofness”.
- References adjusted and cleaned-up.
- Some other editorials and nits.

# Applicability

- New section 2.1 on applicability of DHHMAC for SIP/SDP and H.323 added:
  - MIKEY and MIKEY-DHHMAC are optimized key management protocols and targeted for the purpose of multimedia applications with application-level key management needs under real-time session setup and session management constraints.
  - DHHMAC is applicable for integration into two-way handshake session- or call signaling protocols:

    a) SIP/SDP: encoded MIKEY messages are encapsulated and transported in SDP containers of the SDP offer/answer handshake.

    b) H.323: encoded MIKEY messages are transported in the H.225.0 fast start call signaling handshake (See draft H.235 Annex G).

  - MIKEY-DHHMAC is offered as option to the other MIKEY key management variants.

# Next Steps

- Document ready for WG LC ?
- Not quite: draft-ietf-msec-mikey-dhhmac-03.txt is ahead…
- Launch WG LC in August 2003.

# draft-ietf-msec-mikey-dhhmac-03.txt Ahead

- Section 1: Relationship with other, existing work mentioned.
- Text allows both random and pseudo-random values.
- Clarified that the HMAC is calculated over the entire MIKEY message excluding the MAC field.
- Section 4.2: The AES key wrap method SHALL not be applied.
- Notation aligned with MIKEY-07.
- Exponentiation ** changed to ^.


Thank You!
It's time for Questions...