HMAC-authenticated Diffie-Hellman for MIKEY

IETF #60 San Diego 2004

Steffen Fries
Siemens AG, Corporate Technology, CT IC 3
81730 Munich, Germany
Tel: +49 89 636 53403 E-mail: steffen.fries@siemens.com

draft-ietf-msec-mikey-dhhmac-06.txt

Update & Status

Changes against –05.txt

- Updated draft draft-ietf-msec-mikey-dhhmac-06.txt.
- Changes against draft-ietf-msec-mikey-dhhmac-05.txt:
  - HMAC-SHA1-96 option removed (see section 1.2, 4.2, 5.3).
    This option does not really provide much gain;
    removal reduces number of options.
  - Mandatory IDr added to I_message for DoS protection of the recipient;
    see section 3, 3.1, 5.3.
    This allows the recipient to filter out those (replayed) I_messages that are not targeted for him and avoids the recipient from creating unnecessary MIKEY sessions.
- References updated.

DH-HMAC Security Protocol

Initiator I

Provides DoS protection of the recipient

Responder R

I_message := HDR, T, RAND, [IDi], IDr , {SP}, DHi, KEMAC

R_message := HDR, T, RAND, [IDr], IDi, DHr, DHi, KEMAC

TGK := g^{xy} mod p **TGK := g^{xy} mod p**

→ TGK re-keying security protocol holds analogous enhancement

IPR

- *"…*
  The author believes to be aware of related intellectual property rights currently being held by Infineon.
  Pursuant to the provisions of [RFC-2026], the author represents that he has disclosed the existence of any proprietary or intellectual property rights in the contribution that are reasonably and personally known to the author.
  The author does not represent that he personally knows of all potentially pertinent proprietary and intellectual property rights owned or claimed by the organizations he represents or third parties. …"

- How to handle this situation ?
  Who to submit an entry into the "IETF IPR notices"?