HMAC-authenticated Diffie-Hellman for MIKEY

IETF #61 Washington, DC, 11/2004

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-07.txt

Update

Changes against –06.txt

- Used new RFC boilerplate:
  - changed/moved IPR statement; now at the beginning (see also note well slide),
  - status of Memo,
  - and Intellectual Property Rights section in accordance with RFC 3667, RFC 3668.
- Abstract reworded.
- Note added to section 4.1 explaining how to differentiate between MIKEY and DHHMAC.
- New section 4.4 added that describes the use of the general extension payload to avoid bidding-down attacks;
  Removed description of the bidding-down avoidance mechanism from the threat model in section 5.2.
- IANA considerations section re-written and aligned with MIKEY.
- Open issue on KMID encountered in IANA considerations section; discussion and resolution process is ongoing within MMUSIC WG.
- References updated.
- ID nits removal and editorial clean-up.

Next Steps

- AD review
- (XML/HTTP representations of the .txt are under preparation)

Note well, IPR

- By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

- The author believes to be aware of related intellectual property rights presumably currently being held by Infineon.
  Pursuant to the provisions of [RFC3668], 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.

  [A 3rd party disclosure entry has been submitted to IETF.

  This paragraph (2nd bullet) will be removed from the –08 draft, once the submitted 3rd party disclosure entry will have shown up in the IETF IPR DB.]