HMAC-authenticated Diffie-Hellman for MIKEY

IETF #62 Minneapolis, 03/2005

Steffen Fries, ✉ : steffen.fries@siemens.com

Siemens AG, Corporate Technology, CT IC 3
81730 Munich, Germany

draft-ietf-msec-mikey-dhhmac-09.txt

Update & Status

Changes against –07.txt

- Two new draft versions since last time: -08 and -09
- AD review accomplished: many thanks to Russ

- Feedback from AD review incorporated into -08:
  - added considerations on the possible impact of “PKIX” protocols and operations to end systems with real-time constraints (section 1).
  - added note that DH group is transmitted explicitly but not the parameters g and p; see section 3.
  - added considerations on clock synchronization and timestamps in section 2 and in section 5.3 in the view of consequences on replay protection.
  - references updated.
  - editorial corrections and cleanup.

- -09 changes against -08:
  - “PKIX” removed and replaced by “operations in the context of a public-key infrastructure”.
  - some minor editorials.

Status

- IETF last call completed in February 2005 without any comments raised.
- IETF Status Tracker reports:
  - Status is: In **IESG Evaluation**
  - Placed on agenda for telechat - 2005-03-03 by Russ Housley
- Note well, IPR
  - A 3rd party disclosure entry has been submitted to IETF, see https://datatracker.ietf.org/public/ipr_detail_show.cgi?ipr_id=539

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.

- 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, see

- https://datatracker.ietf.org/public/ipr_detail_show.cgi?ipr_id=539