HMAC-authenticated Diffie-Hellman for MIKEY

IETF #58 Minneapolis 2003

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-04.txt

Update & Status

Changes against –02.txt
Changes against –03.txt

- Two updated drafts produced since Vienna.
- Only editorial changes and clarifications.
- Changes against draft-ietf-msec-mikey-dhhmac-02.txt:
  - Text allows both random and pseudo-random values for x_i.
  - Exponentiation ** changed to ^.
  - Notation aligned with MIKEY-07.
  - 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.
  - Section 1: Relationship with other, existing work mentioned.
- Changes against draft-ietf-msec-mikey-dhhmac-03.txt:
  - RFC 3552 available; some references updated.

Status & Way Forward

- Working Group Last Call during August completed with very little feedback received.
- Some discussion on MSEC mailing list afterwards.
- "Do we need the IETF standardizing yet another DH-based key management protocol ?"
  - ⇨ Yes, there are use cases that leverage the limitations of MIKEY-DHSIGN (PKI dependency, need for PFS, “real-time” capable key management)
- “How does DHHMAC fit into group security?”
  - ⇨ As a registration protocol between group controller and endpoint.
  - ⇨ Point-to-Point characteristic of DH rules out group deployment.
  - ⇨ Applicable for example in group-based IP telephony.
  - ⇨ Common GC and shared key assumption simplifies group setup.
  - ⇨ Shared key infrastructure has different trust model than general PKI.
- Conclusions:
  - Draft should better explain these issues (➔ -05)

Thank You!

It's time for Questions...