

HIP-WG meeting, IETF-64

HIP mobility and multihoming update (draft-ietf-hip-mm-02.txt)

November 8, 2005

Tom Henderson (editor)

Draft authors: Jari Arkko, Tom Henderson,
Pekka Nikander, Greg Perkins, Christian Vogt

Protocol overview

Readdressee

Peer

UPDATE

Contains new LOCATOR (e.g., address, SPI)
Authentication (HMAC and Signature)

Optional:

- Rekey (new SA)
- Generate new KEYMAT

UPDATE, ACK (with nonce)

Mandatory address check
(to prevent DoS attacks)

Optional:

- Rekey, generate new KEYMAT
- Credit-based Authorization

ACK (with nonce)

- Similar, but more complicated, procedures for multihoming
- Interaction with DNS, Rendezvous Servers out of scope

Draft status

- draft-ietf-hip-mm-02.txt presented at last meeting
 - address checks mandatory
 - new security section
 - Credit-Based Authorization added
 - RFC-4101 protocol model added
 - LOCATOR parameter is not differential (always contains all valid addresses)
- No draft changes since last meeting
 - some more implementation experience?

Open issues

- Is the draft too ESP-centric?
 - discussion of how to combine with ESP rekeying could be decoupled
- Policy Considerations and IANA Considerations sections are not yet written

Recommendations

- Gain interoperability experience at IETF 64
- Post -03 draft within the next month
 - pending the discussion any design changes on list
- WGLC shortly after