Updates on RFC5444/NHDP Security

Ulrich Herberg
Thomas Clausen

Updates on draft-ietf-manet-packetbb-sec-09

- Approved!
- In RFC Editor Queue
- 2 DISCUSSes resolved (from Robert Sparks and Stephen Farrell)

Changes since draft-ietf-manet-packetbb-sec-07

- Renamed “Digital Signature” to “Integrity Check Value (ICV)” (to allow for MACs, e.g. HMAC)
- Replaced 1 octet <key-index> to
  1 octet <key-id-length> and <key-id>
- One SHOULD became MUST (“ICV TLVs MUST be restored after calculating the ICV”)
- Reinstated initial registry allocations for time stamps and hash/crypto algorithms (from revision -01)
- Reduced type extension allocation size for “experimental use” from 32 to 4
- Editorial issues

Updates on draft-ietf-manet-nhdp-sec-01

- Updated to accommodate draft-ietf-manet-packetbb-sec-09
- Editorial edits
- No major changes of the specification

TODO for -02:

- Allow for calculating ICVs for addresses within messages (as allowed by packetbb-sec)
- WG LC?