RMT NORM Update

draft-ietf-rmt-pi-norm-revised-13

Brian Adamson

28 July 2009

IETF 75 - Stockholm, Sweden

draft-ietf-rmt-pi-norm-revised-13

- Had addressed IESG Comments
  - Loose use of SHALL/REQUIRE/etc terms
  - Discussion-oriented text tightened to clearer specification on some details
  - Security Considerations improved
  - Removed IANA registry URNs
- New Comments Received
  - Some technical comments on IPSec usage specification and need to specify IPSec version
  - Automated keying options not clear
  - Tim Polk to provide some added clarification
  - Comment on *NormNodeId* assignment not being clear
- Some comments may also apply to ALC “Security Considerations”
- Updated draft in progress

Summary of Main Issues

- NORM Security
  - Some trade-offs between group size scalability and level of assurance
  - Shared IPsec SA (and keys) among receivers allows large group size w/ current IPsec implementation but shared key offers chance one receiver to masquerade as another.
- *NormNodeId*
  - Administrative assignment needed.
  - For SSM operation, *NormNodeId* collisions can't be detected (i.e., as with RTP SSRC ID) since receivers don't hear each other.
  - Revisit earlier proposal to allow *NormNodeId* to be a TLC (type-length-value) encoding and/or flag to indicate use of IPv4/IPv6 source address as NORM "source_id"?