# Multicast Security (MSEC) WG

IETF-57, Vienna

Mon, July 14, 2003

1930-2200 Evening Sessions

# MSEC Agenda

- Agenda Bashing (5min)
- Review of WG Status (T. Hardjono) (15min)
  - Current drafts, recharter and new milestones
  - New drafts
    - Securing Feedback Messages
- GSAKMP Update (H. Harney) (20min)
- MIKEY Update (F. Lindholm) (20min)
- FMKE (S. Josset) (20 min)
- DHHMAC for MIKEY Update (M. Euchner) (20min)
- GKM Architecture (L. Dondeti) (20min)
- Discussion

# Current MSEC drafts

| | |
|---|---|
| Key manag. architecture | draft-ietf-msec-gkmarch-05.txt |
| GSAKMP Light | draft-ietf-msec-gsakmp-light-sec-01.txt |
| GSAKMP | draft-ietf-msec-gsakmp-sec-02.txt |
| GSAKMP Token | draft-ietf-msec-tokenspec-sec-00.txt |
| MESP | draft-ietf-msec-mesp-01.txt |
| TESLA specs: | draft-ietf-msec-tesla-spec-00.txt |
| TESLA intro: | draft-ietf-msec-tesla-intro-01.txt |
| DHMAC for MIKEY | draft-ietf-msec-mikey-dhhmac-02.txt |
| Issues w. IPsec for multicast | draft-ietf-msec-ipsec-multicast-issues-01.txt |
| Tunelled GSAKMP | draft-ietf-msec-tgsakmp-00.txt |
| Feedback | draft-ietf-msec-secure-feedback-00.txt |

# Last Call docs

## Last Call

| | |
|---|---|
| MIKEY | draft-ietf-msec-mikey-07.txt |
| MSEC Arch | draft-ietf-msec-arch-01.txt |

## RFC

| | |
|---|---|
| GDOI | RFC 3547 |
| | |

# Recharter

- Re-charter and New milestoned dates:
  - Approved by ADs – June 2003
- Re-charter:
  - Extend life-time of MSEC to 2004
  - Add new paragraph:

"In addition, as a secondary goal the MSEC WG will also focus on distributed architectures for group key management and group policy management, where for scalability purposes multiple trusted entities (such as Key Distributors) are deployed in a distributed fashion. For this purpose, the Reference Framework will not only describe one-to-many multicast, but also many-to-many multicast."

# New Milestones

| | |
|---|---|
| Done | Working Group Last Call on MIKEY Protocol. |
| Done | Working Group Last Call on MSEC Arch. high level doc |
| Sep 03 | Last Call on GKM-Architecture draft |
| Sep 03 | WG Last Call on DHHMAC for MIKEY [follows MIKEY] |
| Sep 03 | WG Last Call on Data Security Architecture draft. |
| Sep 03 | WG Last Call on GSAKMP protocol |
| Dec 03 | WG Last Call on Security Requirements draft. |
| Mar 04 | WG Last Call on Group Security Policy Arch & Token |
| Mar 04 | WG Last Call on MESP (Multicast ESP) draft. |
| Mar 04 | WG Last call on MESP-TESLA draft. |
| Jul 04 | WG disband or re-charter for other work items |

# MSEC drafts tree