MSEC WG
73rd IETF

Co-Chairs:
Brian Weis
Lakshminath Dondeti
Agenda

• Administriva (5 minutes)
  – Mailing list: msec@ietf.org
  – Blue Sheets

• Document Status
  – Lakshminath/Brian (10 minutes)

• Use of TESLA in the ALC and NORM Protocols
  – Vincent Roca (15 minutes)

• Using Counter Modes with ESP and AH to Protect Group Traffic
  – David McGrew (10 minutes)

• GDOI Update & GDOI Generic MAC Policy
  – Sheela Rowles (15 minutes)
Document Status

• Published since 71st IETF:
  – RFC 5197 (On the Applicability of Various Multimedia Internet KEYing (MIKEY) Modes and Extensions)

• Active Drafts
  – draft-ietf-msec-ipsec-extensions-09
    Status: in Auth48, should be published soon
  – draft-ietf-msec-tesla-for-alc-norm-06
    Status: Author responding to Last Call comments
  – draft-ietf-msec-ipsec-group-counter-modes-02
    Status: Ready for Last Call
Document Status (cont.)

• Expired Drafts
  – draft-ietf-msec-gdoi-update-03
    Status: Authors editing draft
  – draft-ietf-msec-gdoi-srtp-01
    Status: Need to assess support
  – draft-ietf-msec-ipsec-composite-group-01
    Status: Need to assess support
  – draft-ietf-msec-ipsec-tesla-00
    Status: Abandoned?
  – draft-ietf-msec-gkdp-01
    Status: Abandoned?
Document Status (cont.)

• Individual Drafts
  – draft-weis-gdoi-mac-tek-00
    Status: *Update presentation on the agenda*
Milestones

Oct 2008  WG Last Call on Use of TESLA in the ALC and NORM Protocols
Nov 2008  WG Last Call on Using Counter Modes with ESP and AH to Protect Group Traffic
Jan 2009  WG Last Call on Updates to the Group Domain of Interpretation (GDOI)
Mar 2009  WG re-charter for other work items or disband