```
----------------------------------------------------------------------
MSEC WG Session Summary - IETF60
---------------------------------
```

Notable updates

The MSEC WG meeting at IETF-60 was held on Monday 2 August 2004.
(MSEC did not meet at IETF-59).

A number of updates were provided by draft-authors regarding
their current documents. Two notable updates are that
the GSAKMP base draft completed WG Last Call in July 2004,
while the DHHMAC-for-MIKEY draft completed IESG Last Call in May.

With regards to GSAKMP, it was agreed by the WG that the other
two existing drafts relating to GSAKMP (namely the Policy-Token
draft and the IPsec-mapping-for-GSAKMP draft) will be targeted
for Standards Track.

In addition, it was agreed that MSEC should commence WG Last Call
for the RSA Signatures draft (draft-ietf-msec-ipsec-signatures).

Revised Milestones

With regards to the current MSEC milestones, the MSEC WG has in
fact missed the deadlines for a number of promised documents.
As such, the MSEC milestones will be revised to reflect new
delivery dates. The proposed revised milestone dates will be
delivered to the Security ADs for approval.

Note that the MSEC Charter itself will *not* be modified.

New Work Items

The new milestones will also reflect new drafts that
will be submitted to MSEC and which have been agreed upon
to indeed fall under the scope of MSEC's Charter.

Two of these work items are

- GDOIv2 This draft will look at changes found in IKEv2, and will
  incorporate changes to the GDOI protocol flow addressing some
  security weaknesses found by Cathy Meadows' analyses.
  In addition, the draft may address the use of multiple
  Key Distributors (GCKS), as intended and expressed by the
  existing Charter of MSEC.

- IPsec SA issues in Multicast Security This draft will capture
  the issues and discussion regarding IPsec SAs in the context
  of secure multicast. Although RFC2401bis reflected some changes
  requested by the MSEC WG, the MSEC community felt that the
  background, motivations and problems with the use of IPsec SAs
  in multicast needed to be documented and explained.
  As such, this draft is aimed at Informational.