MSEC WG status

Brian Weis

IETF-62, Minneapolis, MN

Mar 10, 2005

Agenda

- **Agenda bashing**

- **WG Status review (Brian Weis)**

- **2401bis and multicast issues (AD discussion - Russ Housley)**
  Document(s): 2401bis I-D and RFC 3740

- **Additional mode of key distribution for MIKEY (F. Audet/L. Dondeti)**
  Document(s): draft-ignjatic-msec-mikey-rsa-r-00.txt

- **MIKEY - using elliptic-curve methods (Mitch Blaser/Andy Milne)**
  Document(s): None posted yet.

- **Update on DHHMAC draft (S. Fries)**
  Document(s): draft-ietf-msec-mikey-dhhmac-09.txt (in IESG review)

- **Bootstrapping TESLA draft (S. Fries)**
  Document(s): draft-ietf-msec-bootstrapping-tesla-00.txt (finished WGLC)

Since the last meeting …

- The following I-Ds have finished WGLC
  - draft-ietf-msec-newtype-keyid-01.txt
  - draft-ietf-msec-srtp-tesla-03.txt
    - Updates in progress?
    - Mark Baugher has the token (according to Elisabetta)
  - draft-ietf-msec-bootstrapping-tesla-00.txt
    - The last call email had an error that was corrected
    - ***Does anyone have any issues with this I-D?***
- The following I-D has finished IESG last call
  - draft-ietf-msec-mikey-dhhmac-09.txt
    - Russ's feedback: The IANA Considerations section could be a bit more clear.

Drafts' status

• draft-ietf-msec-gkmarch-08	2004-06-10	Active	RFC Ed Queue
• draft-ietf-msec-tesla-intro-04	2004-12-08	Active	RFC Ed Queue
• draft-ietf-msec-gsakmp-sec-07	2005-01-12	Active	IESG Evaluation
• draft-ietf-msec-ipsec-signatures-04	2005-02-15	Active	IESG Evaluation - Defer
• draft-ietf-msec-mikey-dhhmac-09	2005-02-02	Active	IESG Evaluation

Lakshminath/Ran will be forwarding these to the ADs

• draft-ietf-msec-bootstrapping-tesla-00	2005-01-18	Active	in WGLC/finished
• draft-ietf-msec-newtype-keyid-01	2005-02-14	Active	Finished WGLC
• draft-ietf-msec-srtp-tesla-03	2005-02-14	Active	Finished WGLC

Drafts' status

Lakshminath & Ran will put deadlines on these

• draft-ietf-msec-tesla-spec-00	2002-10-30	Expired	AD is watching – Needs Update
• draft-ietf-msec-gdoiv2-01	2004-10-26	Active	Needs Update

Policy: need status update from authors

• draft-ietf-msec-policy-token-sec-02	2005-03-08	Active	ID Exists
• draft-ietf-msec-tokenspec-sec-00	2003-02-24	Expired	ID Exists
• draft-ietf-msec-gspt-02	2003-08-19	Expired	ID Exists

Need a rough idea from the authors on how long these will take

• draft-ignjatic-msec-mikey-rsa-r-00	2005-01-28	Active	NEW
• draft-ietf-msecmikey-ecc-00	(to be submitted)		NEW

Do we need to revive these considering Russ's presentation?

• draft-ietf-msec-mesp-01	2003-03-21	Expired	Dead
• draft-ietf-msec-ipsec-multicast-issues-01	2002-12-23	Expired	ID Exists

Back to the agenda

- **Agenda bashing**

- **WG Status review (Brian Weis)**

- **2401bis and multicast issues (AD discussion - Russ Housley)**
  Document(s): 2401bis I-D and RFC 3740

- **Additional mode of key distribution for MIKEY (F. Audet/L. Dondeti)**
  Document(s): draft-ignjatic-msec-mikey-rsa-r-00.txt

- **MIKEY - using elliptic-curve methods (Mitch Blaser/Andy Milne)**
  Document(s): None posted yet.

- **Update on DHHMAC draft (S. Fries)**
  Document(s): draft-ietf-msec-mikey-dhhmac-09.txt (in IESG review)

- **Bootstrapping TESLA draft (S. Fries)**
  Document(s): draft-ietf-msec-bootstrapping-tesla-00.txt (finished WGLC)