

# Keying and Authentication for Routing Protocols (karp)



<http://www.taipeitimes.com/News/biz/photo/2003/10/17/0000063738>

IETF 82

# Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

# Agenda

## **Administrivia** (5 minutes)

- Scribes (Meeting Minutes & Jabber)
  - Many thanks to Richard Graveman, for volunteering to take meeting minutes!
  - Many thanks to Melinda Shore for volunteering to Jabber Scribe
- Blue Sheets

## **Welcome & Document Status** - Chairs (15 minutes)

### **Core Documents**

- *Design Guide Frameworks discussion* – Chairs & WG (15 minutes)
- *Database of Long-Lived Symmetric Cryptographic Keys* – Tim Polk (15 minutes)
- *Operations Model for Router Keying* – Sam Hartman (15 minutes)

### **Routing Protocol Analysis Documents**

- *KARP IS-IS security gap analysis* - Uma Chundauri (15 minutes)

### **Automated Key Management for Routing Protocols Using TCP**

- *Using IKEv2 with TCP-AO* - Uma Chundauri (15 minutes)
- *Key Management for Pairwise Routing Protocol* - Dacheng Zhang (15 minutes)

### **Automated Key Management for Multicast-Based Routing Protocols**

- *The Use of G-IKEv2 for Multicast Router Key Mgmt* - Paulina Tran (15 minutes)

# Current WG Drafts

## **draft-ietf-karp-design-guide-07**

*Status:* IESG Evaluation - Defer::AD Followup

## **draft-ietf-karp-threats-reqs-03**

*Status:* Waiting for AD Go-Ahead::Revised ID Needed

## **draft-ietf-karp-ospf-analysis-02**

## **draft-ietf-karp-routing-tcp-analysis-00**

*Status:* I-D Exists. Advancement blocked on approval of design-guide and threats-reqs.

## **draft-ietf-karp-crypto-key-table-02**

*Status:* I-D Exists. New version needs review.

## **draft-ietf-karp-ops-model-01**

*Status:* I-D Exists. New version needs review

# Design Guide Frameworks discussion

- One outstanding DISCUSS from Russ H.

“Since we know that manual key management must be supported, the KARP WG has decided to specify a crypto key table. Manual key management is populating the table, but this needs to be accomplished using an interface that protects the keying material from disclosure or alteration.

In addition, we want to specify automated key management. A protocol to automatically populate the crypto key table will be used. Several cases need to be considered:”

- Pairwise keys
- Group Keys
  - distributed by a key center
  - group keying protocols

# Responses to the DISCUSS

- Manav Bhatia
  - “... we have not had any discussions on whether this is the FINAL approach that we are taking. I think its too premature to commit to this and the design guide should remain oblivious to a solution that has not even been debated in the WG.”
- Several WG members agreed
- A couple WG members disagreed
- We need Consensus to progress this and a number of other documents....

# Question before the WG:

- The KARP Working group agreed to adopt the Key Tables abstraction as a representation of the interface between the routing protocols and manual or automatic key management.
- The question before the WG is whether it is appropriate for the design guidelines to reference this, and to expect that protocol specific efforts will look carefully at the relevance of the key tables work to the specific case.