

Keying and Authentication for Routing Protocols (karp)

IETF 79

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)
 - Blue Sheets
- **Welcome & Progress Report** - Chairs (10 minutes)
- **KARP Design Guidelines** - Gregory Lebovitz (15 minutes)
- **KARP Threat Analysis and Requirements** - Gregory Lebovitz (15 minutes)
- **Database of Long-Lived Cryptographic Keys** - Tim Polk (20 minutes)
- **Operations Model for Router Keying** - Sam Hartman (20 minutes)
- **Multicast Router Key Management Protocol (MRKMP)** - Sam Hartman (20 minutes)
- **Automated Security Association Management for Routing Protocols** -Yinxing Wei (15 minutes)

Progress Report

Current WG Drafts

- Two KARP WG I-Ds have been updated, and need reviews
 - draft-ietf-karp-design-guide-01
 - draft-ietf-karp-threats-reqs-01
- We can't move very much further without reviews, and a rough consensus!
- One KARP WG I-D is on hold until other directions are set
 - draft-ietf-karp-framework-00

Progress Report

Individual Drafts

- Need to get consensus on direction
 - Key tables, as a tool for separating the process of key agreement from the routing protocol
 - If consensus can be had for key tables, we then can consider guidance on how to use the key tables (the “operations model”)
 - We also will be hearing some advance key agreement ideas