

Keying and Authentication for Routing Protocols (karp)

IETF 87

**Koi carp
stepping stones**
Botanischer
Garten Berlin

Photo courtesy of
TripAdvisor



Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

The brief summary:

- ❖ **By participating with the IETF, you agree to follow IETF processes.**
- ❖ **If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.**
- ❖ **You understand that meetings might be recorded, broadcast, and publicly archived.**

For further information, talk to a chair, ask an Area Director, or review the following:

BCP 9 (on the Internet Standards Process)

BCP 25 (on the Working Group processes)

BCP 78 (on the IETF Trust)

BCP 79 (on Intellectual Property Rights in the IETF)

Agenda

Administrivia (5 minutes)

- Scribes (Meeting Minutes & Jabber)
 - We still need a Scribe and a Jabber Scribe
- Blue Sheets

Welcome & Document Status - Chairs (10 minutes)

Core Document

- *Database of Long-Lived Symmetric Cryptographic Keys* – Sam Hartman/Dacheng Zhang (10 minutes)

Routing Protocol Analyses

- *Analysis of Bidirectional Forwarding Detection (BFD) Security According to KARP Design Guide* – Mahesh Jethanandani (15 minutes)
- *Analysis of LMP Security According to KARP Design Guide* – Mahesh Jethanandani (15 minutes)
- *Analysis of RSVP-TE Security According to KARP Design Guide* – Dacheng Zhang (15 minutes)

Key Management

- *Authentication, Authorization and Policy Management for Routing Protocols* – Dacheng Zhang (25 minutes)
- *Secure Transport for PCEP*– Diego Lopez (15 minutes)

New RFC

- RFC 6952
 - Analysis of BGP, LDP, PCEP, and MSDP Issues According to the Keying and Authentication for Routing Protocols (KARP) Design Guide

Current WG Drafts

draft-ietf-karp-crypto-key-table-08

Status: IESG Evaluation (Telechat: 2013-08-15)

draft-ietf-karp-ops-model-07

Status: In IETF Last Call

draft-ietf-karp-isis-analysis-00

Status: I-D Exists. Ready for WGLC

draft-ietf-karp-bfd-analysis-00

Status: I-D Exists. Authors aware of one issue, after which it should be ready for WGLC

Related Drafts (1)

draft-mahesh-karp-rkmp-04

Status: Call for WG adoption made

draft-chunduri-karp-kmp-router-fingerprints-03

Status: Call for WG adoption made

draft-mahesh-karp-rsvp-te-analysis-00

Status: Not a new document, but needs review

draft-bhatia-karp-pim-gap-analysis-00

Status: Expired. May need additional authors to help complete it

draft-atwood-karp-aapm-rp-00

Status: New ID, needs review

draft-mahesh-karp-imp-analysis-00

Status: New ID, needs review

Related Drafts (2)

draft-tran-karp-mrmp-02

Status: Expired. Pending multicast key management architecture discussions

draft-atwood-karp-akam-rp-03

Status: Not clear there is interest by the WG

draft-chunduri-karp-using-ikev2-with-tcp-ao-05

Status: Authors have asked to call for WG adoption

Charter Goals Review

- We have I-Ds proposals matching for each charter item, but we have moved to make them all are WG documents.
 - Many of protocol analyses individual I-Ds have been reviewed and do not appear to have any controversy.
 - The chairs need your help in getting these documents reviewed, accepted as WG items, and through WGLC.
- Automated key management will take a bit longer, but progress is needed.
 - Please review the two documents that have been requested to be adopted and state your opinion
 - Subsequent KM work also needs to progress

Now, for our first presentation ...