



RSVP Authentication

draft-turner-rsvp-auth-update

S. Turner, L. Berger, M. Jethanandani,
K. Patel, D. Zhang – TSVANG IETF 87



Initial Purpose

- o Add algorithm agility
 - o 1st attempt == FAIL
 - o Explicit indication not required
 - o Key identifier is all you need
- o Specify a new MTI (mandatory to implement), likely HMAC-SHA-foo.



Revamp

- Explain how algorithm agility is supported using key identifier and KARP key table.
- Specify a new MTI (mandatory to implement), likely HMAC-SHA-foo.