Media Description for IKE in SDP

draft-saito-mmusic-sdp-ike-01

Makoto Saito
ma.saito@nttv6.jp

Dan Wing
dwing@cisco.com
Purpose

• Setting up IPsec (IKE) Using SIP
  – VPN to a home router (or NAT device), etc.

- Remote Client
- SIP Proxy
- Home Router
- Home Network

1. INVITE Transaction
2. IKE (Media Session)
3. Validate Fingerprint of Certificate
4. Tunnel Mode IPsec
Proposals

• Exchange Fingerprint of Self-Signed Certificate for IKE Authentication
  – Same Concept as Comedia-tls (RFC4572)
    • a=fingerprint
  – SIP Identity (RFC4474) can be used for Integrity of SDP

• New Media Format Description “IKE”
  m=application 500 UDP IKE (IKE over UDP)

• New Attribute “udp-setup”
  – Similar to Comedia (RFC4145)
    a=udp-setup:active (IKE Initiator)
    a=udp-setup:passive (IKE Responder)