ZRTP

draft-zimmermann-avt-zrtp-01.txt

Philip Zimmermann prz@mit.edu
Alan Johnston alan@sipstation.com
Jon Callas jon@pgp.com

Goals of ZRTP

- Perfect forward secrecy
- Provide confidentiality to unicast voice conversations
- No reliance on signaling for authentication or key management
- No use of certificates or PKI
- Opportunistic encryption
- Fully compatible with existing VoIP endpoints
- True Peer-to-Peer Architecture (SIP P2P BOF, etc.)
  - No servers needed
- Can be implemented as "bump in stack" and thus deployed *immediately*
  - Running code

Design of ZRTP

- Extend RTP to add key management for SRTP
- Message exchange begins with RTP (after signaling exchange and after ICE)
- Ephemeral DH key agreement with hash commitment
- Short Authentication String (SAS) used for MitM protection
- Key continuity using cached secrets between calls

Next Steps

- Next version will have complete Security Considerations section
- Publication as Informational RFC?

ZRTP Operation