

VoIP signaling requirements
draft-jacobs-signaling-security-requirements-00.txt

- Multi-protocol: SIP, MGCP, H.248
[expect signaling of a single VoIP call
over multiple protocols]
- Broad, includes known requirements and less considered
requirements. Does not fit in any one WG
[scale, key handling, identity, configuration, ops]
- Initiated after attempt to manage keys securely
for IPsec SAs in a carrier context
[Symmetric session key generation, NATs,
linkage with application level security]
- Keying in the context of common usage
is the primary difficulty
[low-bit depth keys, storage, session key setup
mutual identity, device proxy keys]