IKEv2-based Shared Secret Key for O/TWAMP

draft-ietf-ippm-ipsec-04

Kostas Pentikousis (Ed.), Yang Cui , Emma Zhang

IETF 90

Toronto, Canada

Draft Updates since IETF 89 (-03)

- Single option for shared secret key derivation
  - Shared secret key = PRF(SKEYSEED, "IPPM")
  - String "IPPM" comprises four ASCII characters
- Cover the case where both O/TWAMP client and server support IKEv2, but there is no current IKE SA
  - Client initiates the establishment of the IKEv2 SA and selects the mode which supports IKEv2.
  - Alternatively, the client proceeds with the modes defined in RFC4656/RFC5618
- New section 4.4 for O/TWAMP over an IPsec tunnel
- Clarifications and several editorial changes
  - An explanation that eNB and SeGW are 3GPP LTE nodes

WGLC Comments

- No non-supportive feedback so far
- Steve Baillargeon’s comments (in -04):
  - Title change to “IKEv2-based Shared Secret Key for O/TWAMP“—done
  - Highlight benefits of new mode—under discussion on mailing list
  - Expected behavior when IKEv2 SA is rekeyed is not clear enough?
  - Do we need 3 new modes? —WG decision?

Way Forward

- Feedback from WG during the meeting and on the mailing list
- WGLC conclusion