Provisioning Message Authentication Key for PCP using PANA (draft-ohba-pcp-pana-00)

Yoshihiro Ohba
Yasuyuki Tanaka
Subir Das
Background

• ietf-pcp-authentication-00
  – Defines a message authentication mechanism for PCP using a PCP SA
  – Two approaches are identified for establishing a PCP SA
    • Separate key management based on PANA
    • Inline key management based on EAP over PCP
  – But it only provides an inline key management solution
Objective

• draft-ohba-pcp-pana
  – This draft provides a solution for separate key management using PANA
What is PANA?

- PANA (Protocol for carrying Authentication for Network Access) [RFC5191] is a Proposed Standard for network access authentication.
- PANA transports EAP over UDP.
- PANA is a mandatory security protocol in ZigBee IP.
- Open Sources are available.
Solution (draft-ohba-pcp-pana)

• Architecture
  – PaC on PCP client node
  – PAA on PCP server node

• PANA may be conducted either
  – as part of network access authentication, or
  – dedicated to the PCP usage

• Once PANA SA is terminated, the PCP SA is immediately terminated

PCP_AUTH_KEY (PCP MAC key) = prf+(MSK, "IETF PCP" | SID | KID | PCP_Server_ID)
[SID: PANA Session ID, KID:Key ID]
Questions and feedback?