Provisioning Message Authentication Key for PCP using PANA (draft-ohba-pcp-pana-02)

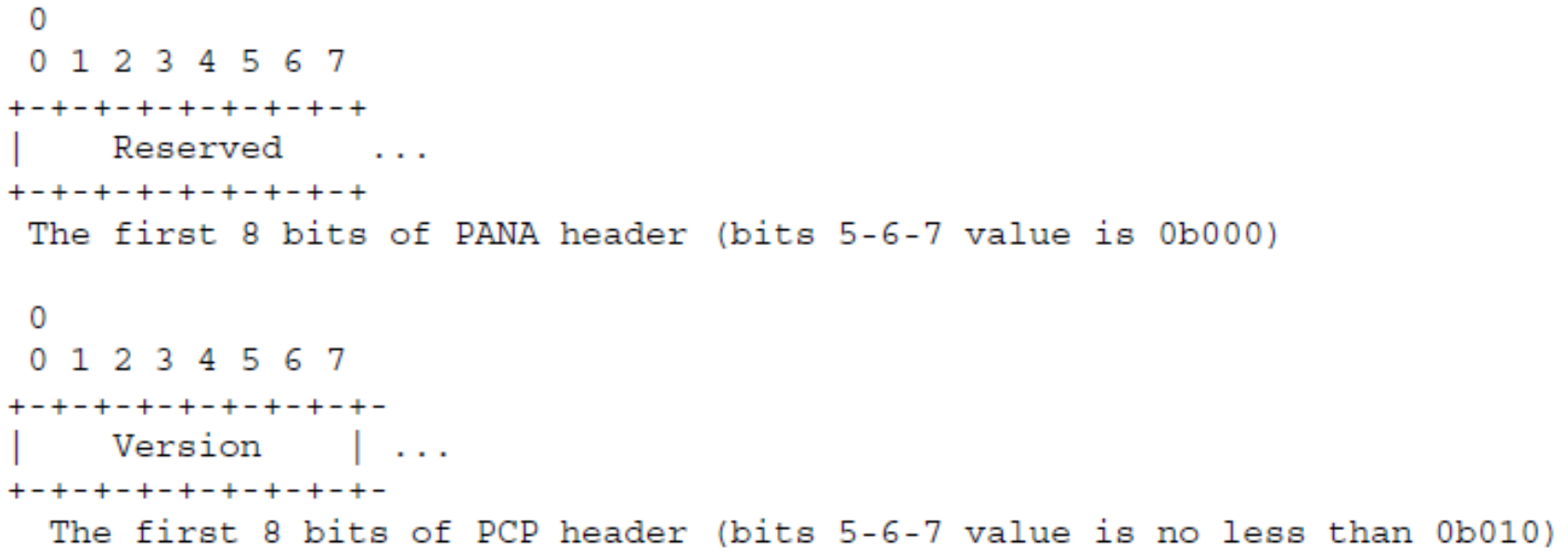
Yoshihiro Ohba
Yasuyuki Tanaka
Subir Das
Alper Yegin

Changes from -00

- Added Alper to authors.
- Defined how to run over PCP port
- Removed PCP server id from key derivation algorithm
- Added EAP channel binding discussion in Security Considerations section.

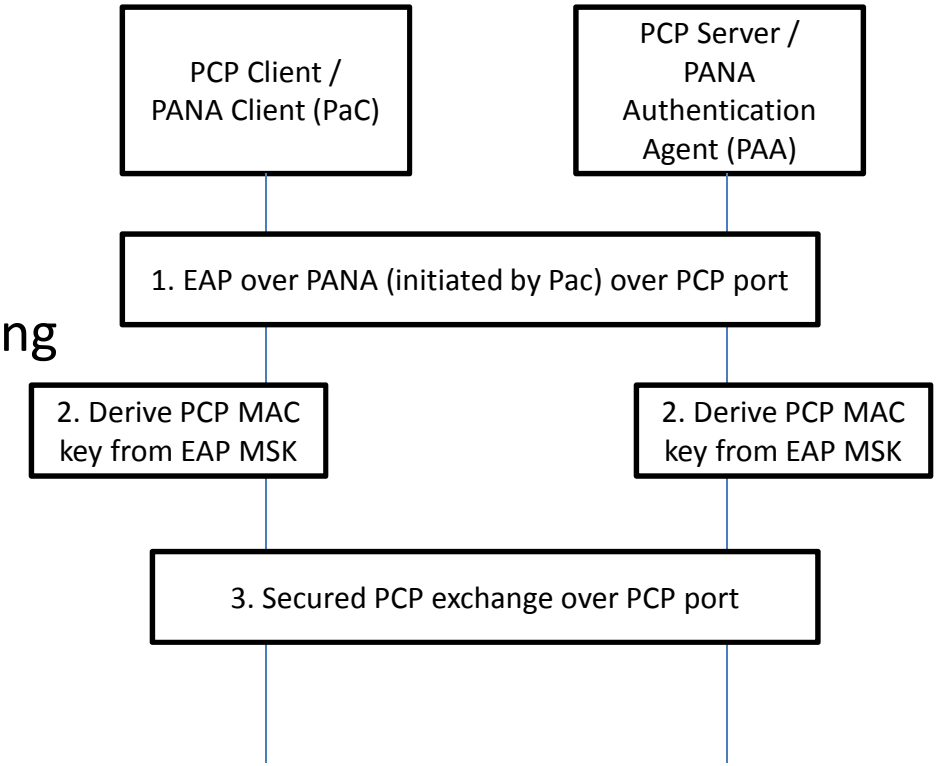
Demultiplexing Approach

- Use well-known PCP port to carry PANA
- Use Bits 5-6-7 to distinguish PANA and PCP
  - To avoid collisions, PCP Version values {8, 16, 24,... 248} MUST NOT be used
  - Note: Alternatively, we can consider allocating 4-bits (hence supporting up-to version 31!)



Solution (draft-ohba-pcp-pana)

- Architecture
  - PaC on PCP client node
  - PAA on PCP server node
- PANA over PCP port is dedicated to the PCP usage
  - Addressing EAP Channel Binding
- Once PANA SA is terminated, the PCP SA is immediately terminated



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

Comparison with tunneling approach

- Encapsulation/tunneling approach:
  - Pros: ???
  - Cons:
    - Encapsulation overhead
    - Tight coupling of PCP and PANA is needed.
      - Some workaround is needed to carry a PCI (PANA-Client-Initiation) message which does not fit PCP's request-response type messaging.
      - Double integrity protection can happen after establishing a PCP SA, where a PANA message carried in the PCP message is protected by a PANA AUTH AVP and the PCP message itself is protected by a PCP Authentication Tag. Avoiding double integrity protection requires more changes to PANA and PCP

- Demultiplexing/Side-by-side/port-sharing approach:
  - Pros:
    - No encapsulation overhead
    - Loose coupling of PCP and PANA
  - Cons: ???

Summary

- The proposal re-uses well-defined and interoperable protocol , allowing specification & code reuse / sharing to carry EAP over UDP for different purposes

- We believe our proposal is ready to make a decision on PCP authentication solution

Questions and feedback?