networkRADIUS

Session identifiers

FOR FAST RE-AUTHENTICATION

ALAN DEKOK IETF 104

THE PROBLEM

- EAP-Session-ID has not been defined for fast re-authentication for
  - EAP-SIM
  - EAP-AKA
- And no Session ID derivation was defined for:
  - EAP-AKA’ (RFC 5448)
  - PEAP

WHAT’S NEEDED

- Vendor EAP methods are likely to have the same problem, too
- Session-Id derivation is needed for ERP (RFC 6696) and FILS (IEEE 802.11ai)

PROPOSAL

- Based in Jouni Malinen’s comments to the EMU mailing list:
- EAP-AKA Session-Id = 0x17 || NONCE_S || MAC
- EAP-AKA’ Session-Id = 0x32 || RAND || AUTN

  Session-Id = 0x32 || NONCE_S || MAC
- EAP-SIM Session-Id = 0x12 || NONCE_S || MAC
- PEAP Session-Id = 0x19 || client.random || server.random

UPDATES

- Updates 5247 (EAP key management framework)
- Should also update
  - RFC 4186 (EAP-SIM)
  - RFC 4187 (EAP-AKA)
  - ~~RFC 5448 (EAP-AKA’)~~ handled by RFC5448bis
  - RFC 5247 (PEAP)

QUESTIONS?