EAP-SIM and EAP-AKA
56th IETF

Henry Haverinen
(henry.haverinen@nokia.com)
Jari Arkko
(jari.arkko@ericsson.com)
Joe Salowey
(jsalowey@cisco.com)

Overview

- EAP methods based on GSM credentials
  - Support for SIM and USIM (AKA) credentials
  - Uses standard SIM and USIM cards.
  - Generates 128 bit keys, has optional fast reconnect and identity privacy support

EAP-SIM Status

- draft-haverinen-pppext-eap-sim-10.txt
- Clarifications on identity handling
- Aligned key derivation terminology and distribution with EAP-TLS
- Security Considerations Updated
- No Known issues remain

EAP-AKA Status

- draft-arkko-pppext-eap-aka-09.txt
- Clarifications on identity handling
- Aligned key derivation terminology
- No Known issues remain

Moving Forward

- Required by 3GPP for R6 ~ June 2003
  - Some existing implementations and deployment
  - Enough feedback already or more needed?
  - The goal is informational RFCs