The ESA Process

Frank Quick

QUALCOMM Incorporated

Vice Chair, TR-45 AHAG

Notice

-
- The information contained in this contribution is provided for the sole purpose of promoting discussion within the TIA and is not binding on the contributor. The contributor reserves the right to add to, amend or withdraw the statements contained herein.
-
-
-

ESA

- Enhanced Subscriber Authentication
- Replacement for the older IS-54 authentication procedures (CAVE)

Need for ESA (1)

- CAVE offers only 56 bits security
  - Short key
  - Known weaknesses
- ESA to provide stronger authentication
  - Increased key size (128 bits)
  - Stronger, publicly proven hash function

Need for ESA (2)

- False base station attacks identified
  - Disabling voice privacy
  - Obtaining private identity information
- ESA will provide bilateral authentication
  - IMT-2000 requirement

Stronger Authentication

- Hash function candidates considered:
  - MD5
  - SHA-1
  - KT proposal (MD4-based)
  - Advanced Hash Algorithm
- TR-45 has selected SHA-1
  - 128 bits for all keys

ESA Feature Summary

- Stronger Mobile Station authentication and key generation algorithm
- Larger authentication keys
- Authentication of Base Station commands

ESA Proposals

- **Lucent: symmetric key with SSD-like intermediate key**
- **AKA: symmetric key with triplet-like AV**
- **Certicom: asymmetric (“public”) key, optional key certification**
  - **Withdrawn**
- **CipherIT: asymmetric (“public”) key, with implicit certification**
  - **Not recommended**

ESA Process

- **Select one of the four ESA key agreement protocols**
  - **TR-45 has selected AKA**
- **Then (in parallel to the extent possible):**
  - TR45.2 develops network protocols
  - AHAG recommends use of SHA-1 within AKA
  - TR45.1, TR45.3, TR45.4 and TR45.5 develop signaling to support the network protocols
  - TR45.6 and TR45.7 provide guidance in their areas of expertise

ESA Standards for 3GPP2

- Core AKA: 3GPP → T1 or TIA
- ANSI-41 MAP: 3GPP2/TR45.2
- SHA-1: 3GPP2/AHAG
- Air interfaces: TR45.3 (TDMA), 3GPP2/TR45.5 (CDMA)
- A interface: 3GPP2/TR45.4