S3-040626

Status of AKA in TIA Standards

Frank Quick
Chair, TIA TR-45 AHAG
QUALCOMM Incorporated

8 July 2004, Acapulco, Mexico

Contents

- **Status of AKA standards in TIA**
- **Status of the AKA Joint Control Agreement**

AKA in TIA Standards

- **TIA-946 Enhanced Cryptographic Algorithms**
- **TIA-136 TDMA air interface specifications**
- **TIA/EIA/IS-2000 CDMA air interface specifications**
- **PN-3-4393 (3GPP2 X.P0006) includes AKA support in the ANS-41 network**

TIA-946

- Published June 2003
- Also published as 3GPP2 specification S.S0055
- Contents:
  - – Enhanced Hash Algorithm
    - » SHA-1 (used as a MAC and as a basic algorithm for AKA)
  - – Authentication and Key Agreement (AKA)
    - » Refers to the ATIS standards corresponding to:
      - 33.102-350
      - 33.103-330
      - 33.105-340
    - » Specifies the use of SHA-1 for functions f0- f5*
    - » Specifies a function f11 for UAK creation
  - – Enhanced Voice and Data Privacy
    - » Specifies the use of AES (Rijndael) for encryption in CDMA

AKA Functions in TIA-946

- Same as in 3GPP TS33 series:
  - f0: RAND generation
  - f1: MACA generation
  - f1*: MACS generation
  - f2: RES & XRES generation
  - f3: CK generation
  - f4: IK generation
  - f5: AK generation
  - f5*: AKS generation
- Additional functions:
  - f11: UAK generation
- Non-AKA functions:
  - GSM triplet generation from Shared Secret Data
  - 2G key generation from 3G keys (e.g. CMEAkey from CK)
  - Key strength reduction (for export/import)

UAK Usage

- **Purpose is to combat the “rogue shell” threat:**
  - **User inserts UIM into a borrowed phone**
  - **The phone retains the CK and IK and makes calls after the UIM is removed**
- **To prevent this, a special key called UAK is optionally created during AKA.**
- **UAK is retained in the UIM**
- **On the network, UAK is a separate, optional parameter, which may be sent along with the AV**
- **If the visited system receives UAK from the home system, UAK is used to encrypt all MACs on mobile-generated signaling messages**
  - **Since the encrypted MAC can only be computed in the UIM, this can be used to prove the UIM is present when the message is formed**

Other Standards

- **Current versions of TDMA (TIA-136) and CDMA (TIA/EIA/IS-2000) support AKA as an option.**
  - **The “2G” authentication based on the CAVE hash algorithm is still the only authentication and key management method in use**
  - **52-bit attacks on CAVE have been claimed, but still no evidence of practical attacks**
- **PN-3-4393, providing network support for AKA is (still!) not published**
  - **Expected publication by the end of 2004**
  - **Network support for AKA is not likely for another two years**
  - **Carriers interested in AKA, but not ready to implement it**

AKA Joint Control Agreement

- **Approved by TIA TR-45 in March 2001**
- **Provides for joint control of:**
  - **TS 33.102:**
    - » **Clause 6.3 *Authentication and Key Agreement***
  - **TS 33.103:**
    - » **Clause 4.2.2 *Authentication and Key Agreement (AKAUSIM)***
    - » **Clause 4.5.3 *Authentication and Key Agreement (AKASN)***
    - » **Clause 4.6.1 *HLR/Authentication Centre***
  - **TS 33.105:**
    - » **Clause 5.1 *Authentication and Key Agreement***
- **Provides that:**
  - **SA3 has editorial responsibility for these documents**
  - **SA3 will notify AHAG if substantive changes are made**

Questions

- **Are the jointly-controlled clause numbers still correct?**
- **Are the document revisions referenced in TIA-946 still applicable?**
- **Is there any additional material that might be considered for joint control?**
- **Any other issues?**