3GPP TSG SA WG3 Security — S3#12 **S3-000233**
12 April, 2000
Stockholm, Sweden

Source: **TR45.2 / TR 45 AHAG**

To: **TSG SA WG3**

Title: **TR-45 AHAG AKA Issues**

Cc:

Contact Person: Christopher Carroll, Chair TIA TR-45 Adhoc Authentication Group (AHAG)
E-mail: ccarroll@gte.com
Tel: +1-781-466-2936

TR-45 AHAG AKA Issues

The TR-45 AHAG has identified several areas of discussion with 3GPP TSG SA WG3, including recommendations to optimize the 3GPP AKA mechanism for TR-45 networks.

Home Control of AKA

1) Recommend that 3GPP add signaling to allow the HLR to revoke the current Authentication Vector (AV) and thereby causing an AV update. It's recommended that this ability be independent of the ability to revoke a registration.

2) Recommend that the Home System have a mechanism to control the duration of the Security Association (SA).

3) Recommend that the Serving Network (SN) report the failure of any authentication and, at the HLR's option, the success of the 3GPP AKA procedure.

R-UIM Privacy and Authentication Key Security

TR-45 is concerned with the potential vulnerability of passing privacy and authentication information (IK and CK) from the UIM to a potentially rogue "MS-Shell". The TR-45 AHAG recommends that S3 and the AHAG explore whether the privacy and authentication information need protection or how the vulnerability to a rogue "MS-shell" may be minimized.

Global (Broadcast) Challenge

1) Local Authentication

TR-45 has decided that Broadcast Challenge is mandatory within all ANSI-41 air interfaces for local authentication, and therefore will be mandatory for all mobiles/UIMs operating in ANSI-41 air interfaces.

2) Initial Registration

TR-45 is currently debating the issue of using Global Challenge on initial registrations to speed up the access process and minimize system loading on TR-45 traffic channels. For this reason, TR-45 is considering whether to use 3GPP AKA for Enhanced Subscriber Authentication (ESA), either with minimal changes, as a secondary key (SSD) update procedure, or both.

SHA -1 Algorithm for 3GPP AKA

TR-45 agreed to adopt SHA-1 as the local authentication algorithm for 3GPP AKA within TR-45 networks. Additionally, TR-45 agreed to strongly recommend the use of SHA-1 for 3GPP AKA key agreement within TR-45 networks. TR-45 proposes that 3GPP consider adopting SHA-1 as the default key agreement algorithm for 3GPP networks.

Agenda Proposal

Procedural issues regarding the introduction of contributions and which documents will control the implementation of AKA and how they will be balloted should be addressed.

Other Issues

Coordination of MAP messaging between 3GPP and ANSI-41 networks may be addressed.