3GPP TSG SA WG3 Security — S3#15 **S3-000562**

12-14 September, 2000

Washington D.C., USA

Source: **Motorola**

Title: **AKA and the Rogue Mobile Problem**

Document for: **Discussion**

Agenda Item:

Introduction

A current item of discussion in both AHAG and 3GPP S3 is how the 3GPP AKA security architecture may address the “rogue mobile” attack. In this attack the mobile retains keys upon UIM removal, thus permitting unauthorized network access prior to subsequent authentications.

It is suggested that allocation of a single bit of the Authentication Vector (AV) “Authentication Management Function” (AMF) may permit the use of secondary keys to solve the rogue mobile problem, without the need for additional network-to-network signaling.

Authentication Management Field (AMF)

The AMF is described in draft 3G TS 33.102 V3.5.0 and in draft 3G TS 33.103 V3.3.0. AMF is a 16-bit component of the Authentication Vector (AV). Typical uses of AMF include differentiation of CS from PS operation, and service provider control over AV usage and duration. The AMF is not standardized by 3GPP but is specified by each Home Network (HN).

The AMF is sent to the User Identity Module (UIM) as a component of the “AUTN”, which accompanies the network challenge RAND. Although the AMF is not encrypted, it is protected from tampering by means of the MAC field.

We suggest that 1 bit of the AMF be used by the HN to indicate whether or not an AV may be used as the seed for a secondary key derivation between the UIM and the Serving Network (SN).

Serving Network and Mobile Station Enhancements

An MS and an SN may generate secondary keys if:

Bi-directional signaling, as via a “capabilities” exchange, establishes that secondary key production is possible, and

The UIM provides an indication to the SN that secondary key production is allowed.

This operation requires accommodations in the MS-to-SN air interface but does not require explicit signaling between the HN and the SN.

Proposal for Consideration

The only solution for prevention of “rogue mobile” attacks requires changing keys on a per-call or per-session basis. It has been argued that frequent AKA-based authentications will drive network traffic loads to unacceptable levels. Therefore the use of a secondary key mechanism has been suggested. However, most secondary key mechanisms require a cooperative relationship between the HN and the SN, as in ANSI-41-based environments.

It is suggested that appropriate use of the AMF field may permit the HN to control the use of a secondary mechanism in the serving environment without the need for an HN-to-SN link.