Technical Specification Group Services and System Aspects
Meeting #19, Birmingham, UK, 17-20 March 2003

**TSGS#19(03)0071**

**3GPP TSG SA WG3 Security — S3#27**
**25 – 28 February 2003**
**Sophia Antipolis, FR**

**S3-030161**

| | |
|---|---|
| **Title:** | **LS on: "Requirement to allow IMS access by means of SIM"** |
| **Response to:** | |
| **Source:** | **SA3** |
| **To:** | **TSG-SA, SA1, SA2 , T3, CN1, CN4** |
| **Cc:** | |

**Contact Person:**

| | |
|---|---|
| **Name:** | **Mireille Pauliac (Gemplus)** |
| **Tel. Number:** | **+33.4.42.36.54.41** |
| **E-mail Address:** | **mireille.pauliac@gemplus.com** |

**Attachments:** **None**

### 1. Overall Description:

SA3 studied the proposal from SA1 to allow IMS Access by the means of the SIM. SA3 identified the following impacts due to the use of the SIM for IMS access.

### 1.1 Security threats

SA3 identified security threats for the different mechanisms proposed to allow the use of SIM for IMS access.

<u>Conversion functions</u>

At SA3#26 Oxford meeting, the proposal on "Allowing IMS Access by means of SIM" was discussed.
To study the feasibility of the proposal, conversion functions were introduced to map GSM AKA to IMS AKA.
But, during the meeting, SA3 identified security problems:

- The home network is not authenticated.
- The session keys are limited to maximum 64 bit effective strength, while the use of USIM for IMS access provides 128 bit keys.
  This restriction to maximum 64 bit effective strength session keys applies not just to the protection of IMS signalling but also to the user plane traffic between the UE and the RNC.
- No guaranty of Random Freshness in GSM AKA.

3G security adds countermeasures against real weaknesses in 2G; UMTS AKA provides enhancements over the GSM AKA. And, the use of SIM for IMS access only provides a 2G-security level while IMS is a dedicated 3G service.

In addition, a security requirement in TS 33.102 states that "Mutual authentication is required between the UE and the HN ", which is in contradiction with the security level provided by this option.

<u>EAP-SIM</u>

An LS from SA2 (S3-030008) proposes possible scenarios to allow IMS access by means of SIM and asks SA3 feedback. The first architectural option consists of the conversion version function studied in the previous chapter and the second option proposes to implement EAP-SIM or similar mechanisms.
EAP-SIM provides some security enhancements (network authentication and stronger session keys). However, security threats exist. The EAP-SIM was analysed in the scope of 3G-WLAN interworking WID and some threats were identified, arising from the exposure of (RAND, SRES, Kc). The risk of exposure of (RAND, SRES, Kc) is due to the fact that computations and checks are performed in the EAP client instead of the UICC.

So the well-known threats to Kc in GSM also apply for IMS if the use of SIM is authorised. In addition, this solution requires protocol changes while the REL-5 is frozen.

Moreover, additional significant issues exist due to the use of the SIM.

### 1.2. Additional issues

- SIM access to IMS will introduce an issue concerning the provision of service in case of roaming, as some operators may refuse to allow subscriber with a lower of security in their network. It will then break the continuity of service.
- Support of USIM is mandatory for REL -5 MEs. It has therefore been clarified that all new services starting from REL-5 must rely on USIM implementation.
- Support of SIM by REL -5 is optional; therefore the envisaged solution would not work with all MEs.
- New REL-5 CRs will have impact on implementation of UEs; it will delay their introduction. Core network will be also impacted by those new REL-5 CRs to allow access to IMS by means of SIM.
- The RFC 3310 only specifies the use of IMS AKA (ISIM), which is identical with UMTS AKA. The use of GSM AKA goes beyond the scope of the RFC 3310. This may require interrogation with IETF e.g. through the 3GPP Liaison Officer.
- REL-5 is frozen
- Moreover, if any problems should come from allowing use of SIM functionality then this may impact the image of the whole system.

So, SA3 identified security threats and issues due to the proposal on “allowing IMS by the means of the SIM”.

## 2. Actions:

**ACTION:** None.

## 3. Next SA3 Meeting:

| Meeting | Date | Location | Host |
|---|---|---|---|
| **SA3#28** | **06-09 May 2003** | **Berlin, Germany** | **European ”Friends of 3GPP”** |