**3GPP TSG SA WG3 Security — S3#30** **S3-030599**
**06 - 10 October 2003**
**Povoa de Varzim, Portugal**

| | |
|---|---|
| **Title:** | Liaison statement on IMS AKA: UE populating RAND and AUTN parameters in responding to challenge |
| Response to: | - |
| **Release:** | Rel-5, REL-6 |
| **Source:** | SA3 |
| **To:** | CN1, CN4 |

**Contact Person:**

| | |
|---|---|
| **Name:** | Tao Haukka |
| **Tel. Number:** | +358 40 5170079 |
| **E-mail Address:** | tao.haukka@nokia.com |

**Attachments:** None

### 1. Overall Description:

SA3 would like to highlight that AKA used in IMS accessing authentication is in different form as the UMTS AKA specified in TS 33.102. The former procedure mandates the UE to populate RAND and AUTH (AKA parameters) in Digest response, explicitly in nonce field, when responding the challeng. This covers both the working case where Digest response wraps the RES, as well as the error case where AUTS parameter is sent. RFC3310 provides best description of them. The UMTS AKA, on the other hand, would require UE to send only RES in working case and only AUTS in case of sequence number out of synchronization.

SA3 would like to assure that correct reference RFC3310 is used, and capture these AKA parameters (RAND, AUTH) in corresponding procedures, in their specifications.

### 2. Actions:

**To CN1 and CN4 groups:**

**SA3 kindly ask CN1 and CN4 to check the correct reference RFC3310 is used, and capture these AKA parameters (RAND, AUTH) in correspinding procedures, in their corresponding specifications.**

### 3. Date of Next TSG-S3 Meetings:

| | | |
|---|---|---|
| SA3#31 | 18-21 Nov. 2003 | Munich, Germany |