3GPP TSG SA WG3 Security — S3#30 **S3-030616**
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 access authentication is in different form to the UMTS AKA specified in TS 33.102. The later procedure requires UE to send only RES in working case and only AUTS in case of sequence number out of synchronization. On the other hand, IMS AKA procedure mandates the UE to populate RAND and AUTN (AKA parameters) in Digest response, explicitly in nonce field, when responding the challenge. This covers both the working case where Digest response wraps the RES, as well as the error case where AUTS parameter is sent from UE. RFC3310 provides best description of them.

In the Cx procedure for sequence number out of synchronization, the S-CSCF needs to send the RAND together with the received AUTS from UE, to the HSS. SA3 would like to make it clear to CN1 and CN4 that the S-CSCF should store the RAND, which was sent to the UE and in the case of synchronisation failure send this stored RAND to the HSS. Using the RAND that is returned by the UE could lead to a replay of synchronization failure messages. SA3 would like to inform that a CR to 33.203 is to be agreed upon next meeting to mandate using the local copy of RAND in S-CSCF.

SA3 asks CN1 and CN4 to kindly ensure that it is clear in their specifications that the RAND stored by the S-CSCF is sent to the HSS in the case of synchronization failures.

SA3 also note that CN4 pass the AUTN parameter in additional to AUTS and RAND to the HSS in the case of synchronization failure. SA3 are not concerned about sending this parameter from a security perspective.

.

2. Actions:

To CN1 and CN4 groups:

SA3 kindly ask CN1 and CN4 to ensure their specification capture that the RAND stored by the S-CSCF is sent to the HSS in the case of synchronization failures where necessary.

3. Date of Next TSG-S3 Meetings:

SA3#31	18-21 Nov. 2003	Munich, Germany
SA3#32	09-13 February, 2004	TBD