3GPP TSG SA3 #28 **S3-030279**
Berlin, Germany, 6 - 9 May 2003

Title: DRAFT LS on increasing the key length for GEA3
Release: Release 6
Work Item: GERAN A/Gb mode security enhancements

Source: SA3
To: CN1
Cc:

Contact Person:
Name: Krister Boman
Tel. Number: + 46317474055
E-mail Address: Krister.Boman@erv.ericsson.se

Attachments: None

---

1. Overall Description:

SA3 is currently investigating how to develop suitable, feasible and cost effective security enhancements for GERAN A/Gb mode. The current concrete technical proposals discussed in SA3 have discussed different mechanisms for the PS-domain i.e. the Gb mode. SA3 has came to an agreement that it should be possible for the system to support both a 64 bit key as well as a 128 bit key for GEA3 (GEA3 is specified in TS55.216-55.219). GEA3 has been designed such that it is possible to use different key lengths from 64 to 128 bits. Since SA3 has agreed that it is sufficient that two key lengths are supported by the system, i.e. 64 bits and 128 bits, a new algorithm identifier should be defined. SA3 has proposed that the new algorithm identifier is called GEA4 which is identical to GEA3 but with a 128 bit key.
This should then be possible to be signalled between the terminal and the SGSN in the Attach request as well as the Authentication Request as specified in TS24.008 and TS23.060.

Note: The specifications TS55.216-219 utilises the parameter KLEN for GEA3 as the key length parameter. It could also be possible to define a new field such that the terminal signals the KLEN parameter instead. However since only two key lengths are required SA3 has ruled out this alternative.

2. Actions:

1. SA3 asks CN1 to consider the work that is currently being progressed in SA3 and in particular to give SA3 feedback on the proposals above

3. Date of Next TSG–SA3 Meetings

Meeting	Date	Location	Host
SA3#29	15-18 July 2003	San Francisco, USA	3GPP2
SA3#30	7-10 October 2003	Europe (TBD)	European 'Friends of 3GPP'