3GPP TSG-SA WG3 Meeting #33 **TD S3-040431**
Beijing, China, May 10-14, 2004

Title:	**LS on removal of A5/2 from handsets.**
Response to:	LS S3-040376 on Removal of A5/2 from handsets from GSMA SG
Release:	6
Work Item:	GERAN network access security
Source:	TSG-SA WG3
To:	TSG-SA WG1, T WG1 WG2, and GERAN WG2
Cc:	GSMA SG, DIG

Contact Person:
Name: Charles Brookson
Tel. Number: +44 20 7215 3691
E-mail Address: cbrookson@iee.org

Attachments: None

---

1. Overall Description:

This LS is for action by the above groups. It is suggested that it is most relevant to S1 and T2. It is a response to a LS from GSMA SG [S3-040376] to remove support for A5/2 in the ME and BTS.

SA WG3 agrees that the removal of A5/2 from the ME will be an important way of reducing the effect of the recent proposed attacks.

Background:
The paper describes how, by using a man in the middle technique, this attack may be used to gain knowledge of the encryption key used for one of the stronger A5 privacy algorithms. Although the attack is currently technically complex and expensive to undertake, it is feasible and equipment could emerge to exploit the weakness identified.

Some GSM operators around the world (for export control reasons) currently use A5/2 and are exposed to the published attack. To do nothing would expose GSM network operators, and their subscribers, to the following difficulties:

- Fraud exposure is greatly increased
- Billing integrity is compromised
- Calls on GSM networks can be eavesdropped
- Degradation of network quality experienced by users

The consequences of this latest attack are most serious for the industry with the result that a joint ad hoc group between GSMA SG and 3GPP SA3 (GSM Security Working Group) was convened to examine the implications of the attack and to identify possible countermeasures.

GSMA Security Group has agreed that the removal of A5/2 from handsets and networks is a solution that must be pursued. It is likely that technical solutions, which will require modifications of handsets and infrastructure, will take considerably longer than simple withdrawal of A5/2. The removal of A5/2 from the network BTS is being pursued by the GSMA, as it is an operator issue.

2. Actions:

To: TSG-SA WG1, T WG1 WG2, and GERAN WG2 groups

ACTION: S3 asks the above groups to:

Modify the specifications so as to remove the mandatory support of the A5/2 algorithm from the R6 ME. The R6 ME should only support A5/0 (no encryption), A5/1 and A5/3, and these should be mandatory.

On a review of the existing standards, only the R99 02.07 standard describes the use of the A5 series of algorithms in the ME. It is suggested that this is moved into a current R6 standard, as otherwise there is a risk that a mobile will be incapable of negotiating an algorithm with a network.

Mobile shall support the following algorithms:
Phase 1 MEs have A5/0 and A5/1 algorithms mandatory.
Phase 1+ and Phase 2 MEs have the A5/0, A5/1 and A5/2 algorithms mandatory.
R6 is changed so that all mobiles must have A5/0, A5/1, and A5/3.

3. Date of Next TSG-SA WG3 Meetings:

.

S3#34	06-09 July 2004	Acapulco, Mexico
S3#35	5-8 October 2004	Malta
S3#36	23-26 November 2004	Shenzhen, China
S3#37	February 2005	Australia (TBC)