3GPP TSG SA WG3 Security — S3#34 **S3-040595**

July 6 - 9, 2004

Acapulco, Mexico

TSG-SA WG1 #25 **S1-040627**

Montreal, Canada, 28 June - 02 July 2004 **Agenda Item:**

Title: LS on removal of A5/2 algorithm in Release 6 MEs

Response to: LS (S1040563 [S3-040431]) on removal of A5/2 from handsets.

Source: **SA1**

To: SA3

Cc: GSMA SG, DIG, T2, GERAN2

Contact Person: Kunle Ibidun
Company: Orange
Tel. Number: +44 (0) 7966 461 005
E-mail Address: kunle.ibidun@orange.co.uk

Attachments: None

1. Overall Description:

SA1 thanks SA3 for their liaison statement S1040563 [S3-040431] regarding the so-called man in the middle security flaw in the A5/2 algorithm.

SA1 note that SA3 have requested that CRs are produced to reflect

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.

The encryption requirements for Phase 1, through Release 98 are defined in GSM TS 02.07. The requirements indicate the support of A5/1 and A5/2.
For R99 through to R6 the requirements are stated in document 22.101 in the clause below:

> "The basic mandatory UE requirements are:…
> Support for the execution of algorithms required for encryption, for CS and PS services. Support for non encrypted mode is required;"

SA1 believe that the requirement for Rel-99 through Rel-6 provides the flexibility for SA3 to implement the requirement proposed for R6 and that the selection of specific security algorithms is beyond the scope of SA1.

However SA1 requires that the current security should not be weakened.
For Phase 1 to Rel-98 SA1 does not believe a change is appropriate.

2. Actions:

None

3. Date of Next TSG-SA1 Meetings:

SA1#26	11 – 15 October 2004 Sophia Antipolis, FR	European friends of 3GPP