

3GPP TSG SA WG3 Security — S3#26

S3-020674

19- 22 November 2002

Oxford, UK

Title: LS on introduction and adoption of A5/3 and GEA3

From: GSM Association Security Group

To: 3GPP TSG SA3

Cc: GSM Association TWG

Contact Person: Name: James Moran
Tel. Number: +353 1 289 1821
E-mail Address: jmoran@gsm.org

The GSM Association discussed the document Tdoc S3-020440 regarding support for the new cipher algorithm A5/3 and GEA3 at its meeting held on 18th to 19th September 2002.

The aforementioned liaison statement sought, from handset and infrastructure manufacturers, the expected time scales for the inclusion of the A5/3 and GEA3 algorithms. The aspiration was expressed that equipment containing A5/3 and GEA3 will be available from October 2004.

The GSM Association Security Group endorsed the proposal but expressed the hope that equipment may even be available before October 2004. The Security Group Chair presented this position to the GSM Association Plenary meeting held in Istanbul in October and it received the endorsement of the GSM Association membership there.

The Security Group understands that the GSM Association and ETSI, in their roles as custodians and distributors of A5/3 and GEA3, are currently working towards publication of the algorithms and it is hoped that this work can be brought to a conclusion without further undue delay.

The Security Group is interested to receive any feedback that may have been collated from the manufacturers regarding when, and what type of, infrastructure and handsets are likely to be available.

Replies can be sent to James Moran, Fraud and Security Director, GSM Association.