S3-010260

3GPP TSG SA WG3 Security — S3#18

21 - 24 May, 2001

Phoenix, USA

Liaison Statement

From: TSG-SA3

To: GSM Association SG (Security Group)

Cc:

Subject: Reply to LS on the Development of new A5/3

Contact: Charles Brookson
DTI CII3e
Tel: +44 20 7215 3691
Email: cbrookson@iee.org

Attachments: none

3GPP TSG SA3 received a LS from GSMA SG on the Development of the new A5/3 algorithm.

Work plan for information
3GPP TSG SA3 endorses the attached SAGE work plan and LS. It would like to see any further changes and amendments if these are made.

A5/3 Kc support for 128 bits
3GPP TSG SA3 considered the change of key to 128 bits. It was thought that the change to 128 bits would be complex and difficult, requiring significant changes to standards throughout GSM.

However, 3GPP TSG SA3 would like to point out that 128 bits should be possible in a few years when operators move to a 3G infrastructure, that will be capable of supporting GSM with this key length.