3GPP TSG SA WG3 Security — S3#17 S3-010095
27 February - 02 March, 2001
Gothenburg, Sweden

From: GSMA SG

To: TSG SA WG3

Meeting Number **SG #38**
SG Doc xx/00
Meeting Date **30-31 January 2001**
Meeting Location **Bristol, UK**

Title Request to investigate an extension of the A5 cipher key length

Source **SG**
Date **27th February 2001**

GSMA SG is content that the development of A5/3 now seems to be imminent to start, with the working assumption that the algorithm will be based on the 3G PP block cipher Kasumi.

However, there is a concern among GSM operators that the upcoming A5/3 must be able to exploit the same full key size of 128 bit as the 3G cipher algorithm allows. As GSM infrastructure presently only allows for 64 bit keys, SG would like to ask S3 to initiate an investigation on different ways forward to ensure that a future release of GSM supporting A5/3 can also at the same time support 128 bit keys. Such a study could possibly also investigate in parallell the introduction of other security enhancements for GSM, like network authentication and other countermeasures against false base station attacks.

An introduction of A5/3 without a substantial increase of cipher key length is considered to be of limited value and possibly not worth implementing. SG would like to have the S3 view on this.