3GPP TSG SA WG3 Security — S3#26 S3-020673

19- 22 November 2002

Oxford, UK

Title: **LS regarding the introduction of new example authentication algorithm for GSM**

From: **GSM Association Security Group**
To: **3GPP TSG SA3**
Cc: **GSM Association SCAG**

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

The GSM Association discussed the introduction of the new example authentication algorithm for GSM at its meeting held on 18th to 19th September 2002.

The new authentication and key generation algorithm has been developed and formally delivered to the GSM Association. However, a research paper on Rijndael published in "Crypto" earlier this year delayed publication of the algorithm pending consideration and the Security Group now accepts from ETSI SAGE that the paper does not compromise the algorithm. As the integrity of COMP128-4 has not been affected, the GSM Association will now proceed with publication of the algorithm.

The Security Group also discussed the name for the algorithm and concluded that it should not refer to the COMP128 name series. The result of the deliberations was that the name "GSM Milenage", (which can be abbreviated to "G-Milenage"), be used and Security Group seeks the approval of 3GPP TSG SA3 to officially use this name.

The Security Group looks forward to receiving the views of SA3 in this regard and a response can be sent to James Moran, Fraud and Security Director, GSM Association.