3GPP TSG SA WG3 Security — S3#22 **S3-020164**

25 - 28 February 2002

Bristol, UK

Title: Use of Milenage as the basis for a new GSM A3/A8 algorithm
Source: SA3
To: SAGE
Copy: GSMA SG, ETSI MCC,

Contact Person:
Name: Peter Howard
Tel. Number: +44 1635 676206
E-mail Address: peter.howard@vodafone.com

GSMA SG have recently suggested that Milenage is used as the basis for a new example GSM A3/A8 algorithm to be made available to GSM operators. SA3 endorse this suggestion and recommend that SAGE begin the work to design and evaluate the new algorithm.

SA3 would like to point out that a "GSM mode" of the Milenage algorithm is already defined in the publicly available 3GPP Release 99 specifications. The "GSM mode" is based on the use of conversion functions and was specified so that certain GSM/3G inter-working scenarios could be supported. SA3 see no reason why this mode cannot be considered as a way of creating a new GSM A3/A8 algorithm based on Milenage.

The specification of the conversion functions is given in 3G TS 33.102. In particular, the conversion functions c2 and c3 are used to convert the 3G parameters RES, CK and IK to the GSM parameters SRES and Kc:

c2: $SRES_{[GSM]} = RES^*_1 \text{ xor } RES^*_2 \text{ xor } RES^*_3 \text{ xor } RES^*_4$
c3: $Kc_{[GSM]} = CK_1 \text{ xor } CK_2 \text{ xor } IK_1 \text{ xor } IK_2$

whereby RES* is 16 octets long and RES* = RES if RES is 16 octets long and RES* = RES || 0...0 if RES is shorter than 16 octets, RES^*_i are all 4 octets long and $RES^* = RES^*_1 \| RES^*_2 \| RES^*_3 \| RES^*_4$, CK_i and IK_i are both 64 bits long and $CK = CK_1 \| CK_2$ and $IK = IK_1 \| IK_2$.

Note that in "GSM mode" the $SRES_{[GSM]}$ is calculated using the 3G RES (variable length) rather than the output of the Milenage f2 function (fixed length of 64 bits).

SA3 acknowledge that other, possibly more efficient, solutions are available. However, the re-use of existing 3G implementations as the basis for the definition of a new A3/A8 is seen as a significant advantage.