Report to SMG Plenary

Copy for information GSMA, GSMA SG, SMG2, SA, N2, N1, SMG9

1 Development of A5/3

The GSM2000 working party (a joint working group of SMG10 and GSM Association Security Group) has determined that a stronger version of A5/1 is required. This is endorsed by SMG10.

This is because the present A5/1 has an effective key length of less than 64 bits, having been developed over ten years ago when stronger algorithms were not exportable. Attacks on A5/1 have recently been published, most recently by Adi Shamir 11-14 April 2000. A draft specification of A5/3 is attached for information.

SMG is therefore asked to endorse the development of A5/3 to:

1) produce an algorithm which has an effective key length of 64 bits. This can be handled at the moment within the GSM standards.

2) support a study of the possibility of extending the key length to 128 bits, to bring it to the same standard as 3G. Volunteers are sought to help in this study; indications should be given to the Chairman of GSM2000 (at present Charles Brookson, cbrookson@iee.org). This study will need to look at protocols where Kc is handled, for example MAP, SIM-ME interface and storage in VLR / AuC.