GSM 2000 Security Meeting No. 7
London DTI, 151 Buckingham Palace Road,
15th May 2000

Present:

Charles Brookson	Chairman
Nigel Barnes	
Henri Gilbert	
Reginald Lee	
James Moran	
Stefan Puetz	
James Semple	
Rolf Schnitzler	
Benno Tietz	
Nigel Barnes	

Emails:
Cbrookson@iee.org, Benno .Teitz@d2mannesmann.de, Rolf.schnitzler@d2mannesmann.de. James.semple@certicom.com, james.moran@gsm.org, reginald.lee@oene2one.co.uk, nigel.barnes@motoroal.com, henri.gilbert@nd.franceteleom.fr, ste fan.puetz@t-mobil.de

1 Introduction

The meeting opened with a brief update on the status of work to produce a requirement specification for the new GSM cipher algorithm.

CB advised that contacts had been made with ETSI and Mitsubishi regarding IPR issues and these details had been passed to the GSMA HQ. Budgetary approval was obtained at the recent GSMA Plenary meeting and SMG10 has given approval for the work to proceed. A new version of the draft specification was made available to each delegate reflecting some recently made changes.

JS pointed out that rather than look exclusively at using Kasumi the group should keep an open mind until further announcements are made regarding AES.

JM confirmed receipt of the IPR contact details and advised that HQ aim to have a definitive statement on IPR/ownership issues.

HG, as a point of information, stated UMTS authentication work by SAGE is currently on hold and repeated the urgency for this group to deliver a new cipher algorithm regardless of the fact that Shamir's most recent paper, presented in New York, did not contain any new developments.

2 Legal Export Control Issues

All parties acknowledge that ownership will prove to be a complex issue. The view of the Group is that the GSMA and ETSI should jointly develop the new algorithm and ownership should be shared by both organisations with the algorithm being an ETSI standard available to members of the GSMA. CB undertook to informally ask ETSI about co-funding.

It was agreed that, from the point of view of export control, the algorithm should apply in all countries. In this regard it was agreed that approval of all partners, assuming there are other partners, would be required to avoid a repeat of the 3G situation.

Following discussion on these points it was agreed that these issues would best be addressed in a document to be added to the requirements specification as an informative annex.

3 Review of Current Requirements Specification

The Group reviewed version 0.4 of the specification and each section was gone through. The most significant changes agreed were as follows;

- All references to export control and ownership would be moved to the proposed informative annex
- The language used in the document should be standardised e.g. will and shall
- Exclusive references to the GSMA should be removed pending further legal advice
- The specification should change to reflect the fact that the algorithm may be used for GSM, GPRS and EDGE

It was agreed that a revised draft should be available by 19th May 2000.

4 Algorithm A5

A5/3 development – current status

The project plan was reviewed and the results are shown below.

Time scales	Task
End of this month	Design authority should be GSM2000 Group. SMG10 approval required GSMA approval required
Mid June Dusseldorf	General approval from SA Technical Study by SAGE suggested describing: a) use of Kasumi b) Any other public algorithms (e.g. AES) c) Design of new A5/3 To describe outline work plan for each, assumptions and suitability of algorithms, cost estimate for each option. Report by end of June
End June	Launch of General Project based on SAGE input
End 2000/ start 2001	It was noted that these time scales still held, but the exact finish date depended on the algorithm being used,

5 LS to SAGE

The meeting agreed that a LS should be sent to SAGE seeking a quotation to conduct a brief study on behalf of the group on a number of issues. Topics to be addressed include the following;

- Obtain technical advice on the use of Kasumi, use of other standards and the development of new algorithm from scratch
- Devise a work plan and cost estimate for each option outlined above

It was agreed that it would be ideal if the report could be available by end May 2000.

6 Algorithm A3

The development of a new authentication algorithm was briefly mentioned and it was agreed that while the work objective should not be abandoned the new cipher algorithm is the current priority. It was felt this project could be resurrected later in the year depending on the progress of the cipher algorithm.

7 Minutes of last meeting

The minutes of the last meeting No. 6 were briefly read out by the Chairman and were accepted without comment. It was noted that the action points arising from that meeting were discharged.

8 Dates of next Meetings

3rd July Dusseldorf (11am)
24th August London
19th October London

Action Points

Action Point	Task
AP1/7	JM to ensure HQ responds on legal issue by early June
AP2/7	CB to informally ask ETSI about co-funding
AP3/7	CB to update requirements specification
AP4/7	CB to draft informative annex
AP5/7	CB to send LS to SAGE regarding conduct of study
AP6/7	JM to contact TWG re handset support for A5/3