3GPP TSG SA WG3 Security — S3#15 S3-000619
12-14 September, 2000
Washington D.C., USA

GSM 2000 Security Meeting No. 9
DTI London, UK
24th August 2000

Present:

Charles Brookson, DTI	Chairman
Rolf Schnitzler, Mannesmann	
Benno Tietz, Mannesmann	
James Semple, Certicom	
Nicola Greco, Motorola	
James Moran, GSM Association	

Emails:
Cbrookson@iee.org, Rolf.schnitzler@d2mannesmann.de, Benno.Teitz@d2mannesmann.de, Jsemple@certicom.com, nicola.greco@motorola.com, james.moran@gsm.org

1. Introduction

The Chairman welcomed the delegates to the meeting and each attendee introduced himself to the group before the meeting continued.

2. Minutes of last meeting - 8

The minutes of meeting No. 8 were presented by the chairman and were accepted without comment. The action points were reviewed and it was noted that TWG indicated it did not have sufficient expertise to respond to SG's liaison statement. HQ will continue to study the SAGE public scrutiny documentation.

3. Update

CB advised the meeting that the GSM Association had approved a budget for the development of A5/3 and also agreed to the use of Kasumi for A5/3. The meeting was also advised that SAGE has agreed to take on the necessary work.

4. A5/3 Project Plan

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

Time scales	Task
Mid September	Requirements specification to be finalised

End September	Formal MoU needed between GSMA and 3GPP and Mitsubishi to cover distribution rights on ETSI IPR terms. Formal project plan to be prepared for SAGE.
Mid October	Next meeting to formally approve expenditure at the next GSM2000 meeting.
November	SAGE to start work for delivery in March 2001
Quarter 1 2001	This remains the target to have development of the algorithm completed

5. Press Statement

In approving the use of Kasumi for A5/3 the GSMA Executive Committee indicated that a press release should issue to announce the decision.

Some debate ensued as to whether or not a press statement should be released and one view was that such an announcement could be construed as being an admission that something is wrong with A5/1. It was suggested that, rather than issuing a press release, we could prepare a wording that could be used in the event that it is necessary however it was felt that this would be reactionary.

On the positive side it was pointed out that a press statement could cover off such issues as publication and evaluation of the algorithm, development of third in a possible set of seven cipher algorithms, 2G migration to 3G, need to ease export restrictions, etc.

The meeting agreed to hold off on the publication of a press release until after the next meeting as a number of other matters need to be finalised. In the interim CB agreed to draft a copy.

6. A5/3 Requirements Specification

The latest version available is version 0.7 and CB will make version 0.8 available shortly.

7. Authentication Algorithm

SAGE is developing a sample authentication algorithm for 3GPP that will have an operator variant. The algorithm may be suitable for GSM so it remains to be seen whether or not the GSM Association will need to develop its own. In any event the GSMA has advised that, if necessary, a budget could be made available.

8. Any other business

JM raised the issue of COMP128 support for 64 bit Kc and following a brief discussion it was agreed that a page should be added to the specification to describe how A8 looks for 64 bits. JM agreed to send a copy of the algorithm to CB, which will then be passed to JS who will hack it back up to 64 bits.

9. Dates of next Meetings

18th October London - GSM Association HQ

Action Points

Action Point	Task
9/1	HQ to study SAGE public scrutiny documentation
9/2	HQ to draft MoU between GSMA and 3GPP & Mitsubishi
9/3	Prepare formal project plan for SAGE
9/4	CB to draft press statement
9/5	CB to circulate version 0.8 of requirements specification
9/6	JM to supply JS, via CB, with copy of COMP128-2.
9/7	JM to make arrangements for next meeting in London