11-14 April, 2000, Stockholm, Sweden

GSM 2000 Security Meeting No. 6
London DTI, 151 Buckingham Palace Road,
10th March 2000

Present:

Charles Brookson	DTI
Reginald Lee	one2one
Mike Howie	Vodafone
Rolf Schnitzler	MMO
Benno Tietz	MMO
James Moran	GSMA

1 Minutes of last meeting

The minutes of the last meeting No. 5 were accepted.

1.1 Action Points from Meeting 5

Action Point	**Comment**
AP1/4 Text should be added to the Q&A on security of COMP128-1 and -2	CB has finalised the text, which will be added to the Q&A document. **Done**
AP2/4 Work item for greater than 64bit A5 needs to be taken forward with a liaison statement to SMG10 for a work item to be started with 96 bit keys and 32 bit SRES	SMG plenary approved the extension of the A5 key length to 64 bits. LS sent regarding extending beyond 64 bits. **AP1/6** No positive reply, to be done again
AP3/4 Charles Brookson to remind GSMA that legal advice is still required before tendering process is started	CB sent liaison statement to GSMA but no response has been received. General IPR reviews in progress. JM to chase up as a matter of urgency. **Done, legal advice to be added by JM**
AP4/4 Charles Brookson to get advice from SMG9 about the size of RAM, ROM and timing required for the COMP128-3. Copy to SMG10.	CB sent liaison statement to SMG9 but has yet to receive a response. To be followed up. **AP2/6** No positive reply, to be done again
AP5/4 Extra test data is required for EDGE. SAGE volunteered if possible time was available.	GSMA has approval expenditure and Thomson and BT to be informed to proceed with the work. **Done**

2 Algorithm A5

2.1 GEA Algorithm

It was noted that the GSMA had negotiated with ETSI to distribute GEA2 as well as GEA1 under ETSI rules form Dublin/

2.2 A5 for Railways (EIRENE)

The GSMA confirmed that under the current rules governing the administration of A5 the railways are not entitled to receive a copy, as they are not a member. It was further confirmed that the railways do not qualify for membership.

2.3 A5/3 development

It was decided that it the highest priority was the development of a new A5/3 for this financial year. This was because the recent news on A5/1 meant that we had a little time to develop the new version. It was that thought that the GSM200 group could look after the development process.

There were two possible development routes; the first was to re-use some of the work done on the 3GPP(1) algorithm, KASUMI. This would require close examination of the Intellectual Property issues, but would be more preferable because multi-mode 3G / GSM mobiles would also have the algorithm built in (it took many years for the adoption of A5/2 in mobile).

An approximate project plan is shown below.

Time scales	**Task**	**Issues**
Now March	Produce project plan, terms of reference and specifications	Get agreement GSMA, SMG10, GSMA SG. Appoint design authority.
26 April 2000 GSMA Plenary	Get agreement for money and project plan	
May 2000	Start development: Design Authority	Should have technical advice, and understand if we can use 3G or need to develop a new A5/3. Can we use any existing public algorithms?
September 2000	Finish design of A5/3	
October 2000	External evaluation of A5/3	
End 2000	Finish process	
2001	Publish algorithms	Intellectual Property & Export control concerns need to be addressed

It was thought that A5/3 could be 128-bit algorithm, but be capable of operating in 56 and 64 bit mode. Depending on work to extend the bit lengths in GSM, then 128 could be possible and we should consider ways of using it in that way.

3 Algorithm A3

3.1 New version

The new version will be delayed, as A5/3 was considered more important.

4 Gossip about Algorithms

The new version of Adi Shamir's paper will be published in April, bringing the amount of known plain text needed for an attack to a few seconds.

5 Dates of next Meetings

15th May,	Dublin or London
24th August,	London
19th October,	London

Action Points

Action Point	
AP1/6	Work item for greater than 64bit A5 needs to be taken forward with a liaison statement to SMG10 for a work item to be started with 96 bit keys and 32 bit SRES
AP2/6	Charles Brookson to get advice from SMG9 about the size of RAM, ROM and timing required for the COMP128-3. Copy to SMG10.
AP3/6	CB to circulate A5/3 thoughts to GSMA SG & SMG10 for comment