Security Group
GSM Association

Liaison Statement

Date: 22nd May 2001

From: GSM Association Security Group

To: 3GPP SA3

Subject: Development of new A5/3

The 39th meeting of the Security Group discussed the proposed development of a new GSM cipher algorithm (A5/3) based on Kasumi.

Work plan for information
A copy of the latest SAGE work plan was tabled for consideration and the document was approved with the following clarifications being noted by the meeting;

- A5/3 will be based on Kasumi and work is currently ongoing with ETSI to resolve some outstanding IPR issues. Indications, previously given by all the interested parties, are that IPR will not stand in the way.
- It is envisaged that A5/3 can also be used as GEA3 for GPRS and offer security for EDGE.
- A requirements specification document was previously worked on by GSM2000, a joint working group made up of ETSI SMG9 and GSMA Security Group delegates.
- The work will be undertaken by ETSI SAGE and the work will be managed by the Mobile Competence Centre on behalf of the GSM2000 working party.
- The costs of developing the algorithm will be borne by the GSM Association. After development the algorithm will be co-owned by the GSM Association, 3GPP and Mitsubishi.
- Distribution and publication of the algorithm will be along the same lines as Kasumi in that it will be published on the web to facilitate scrutiny while a notice will be placed on the site that the algorithm is only to be used by public GSM network operators.

The GSM Association appreciates the assistance afforded to it by many groups in connection with this work and looks forward to receiving the endorsement by SA3 of the proposed SAGE work plan.

A5/3 Kc support for 128 bits
SG would also like to ask SA3 to consider the possibility of extending the A5/3 key length to 128 bits.