3GPP TSG SA WG3 Security — S3#12 **S3-000299**

11-14 April, 2000

Stockholm, Sweden

Source: **Vodafone Airtouch**

Title: **Proposed LS on A5/3**

Document for: **Approval**

Agenda Item:

From: 3GPP TSG-SA WG3 / ETSI SMG10

To: ETSI SMG, SMG2, SMG9,
3GPP TSG-SA, TSG-CN1, TSG-CN2, TSG-T3,
GSMA, GSMA SG

Title: Liaison Statement on A5/3

The GSM2000 group[1] have recently produced a requirements specification for a new strong GSM circuit switched encryption algorithm known as A5/3. The intention is to deploy the new algorithm in GSM systems as soon as possible. The requirements specification has been approved by S3/SMG10 for presentation to the GSMA plenary (25-28th April 2000) for approval. The algorithm design work is being funded by the GSMA.

In parallel with the algorithm design, S3/SMG10 intend to start to investigate issues relating to the effective and efficient roll-out of A5/3. It is expected that this work will require the support of the above mentioned groups. An import requirement will be to ensure that A5/3 cannot be bypassed by an active attacker.

It should be noted that the algorithm requirements specification currently allows for key lengths of up to 128 bits. However, for initial deployment it is envisaged that a 64 bit key will be used. S3/SMG10 intend to start work to investigate the support of longer key lengths in future releases of the specifications.

It should also be noted that the algorithm requirements specification currently suggests that the algorithm could also be used for GPRS encryption by using it as a basis for a new GEA algorithm. S3/SMG10 intend to start work to investigate the roll-out of a new GEA algorithm[2].

---

[1] GSM 2000 is a joint ETSI SMG10 / GSMA SG ad hoc group of experts

[2] Note that this activity is separate to the deployment of GEA2.