3GPP TSG SA WG3 Security — S3#37 **S3-050093**
21 - 25 February 2005
Sophia Antipolis, France

ETSI SAGE **SAGE (05) 16**

14 February 2005

Title: Response on key separation for GSM/GPRS encryption algorithms
Response to: LS S3-041146 "LS on key separation for GSM/GPRS encryption algorithms"
Source: ETSI SAGE
To: 3GPP SA3
Cc:

Contact Person:
Name: **Steve Babbage**
Tel. Number: + 44 1635 676209
E-mail Address: steve.babbage@vodafone.com

Attachments: None

Introduction

SA3 have asked SAGE to comment on whether key separation mechanisms should be introduced in the short term to complement the removal of A5/2 from future handsets.

What this response covers

In our response, we in SAGE have limited ourselves to the areas in which we feel we can add specific value. We do not wish to repeat discussions about the effectiveness or viability of possible security mechanisms, which have had lengthy air time in SA3 already and which SA3 are perfectly competent to discuss.

We therefore present here a summary of how resistant we believe the various GSM and GPRS encryption algorithms are to the attacks that may potentially motivate the introduction of key separation mechanisms.

Our assessment of algorithm strengths

It is important to distinguish between two different classes of attack:

- An eavesdropping attack (breach of confidentiality). Recall that an attack using a false base station (but not a real time man in the middle) can retrospectively decrypt ciphertext produced using a strong algorithm, if it can trick the phone into encrypting sufficient data with the same key using a breakable algorithm.
- A fraud attack based on real time dynamic cloning, as is proposed by Barkan, Biham and Keller.

We leave it to SA3 to judge the relative importance of these two attacks.

A5/1	**Eavesdropping:** Against eavesdropping, A5/1 is rather vulnerable. There are a few different published cryptanalytic approaches to attacking A5/1, but for example the attack by Pornin and Stern (in CHES 2000, available online at http://www.di.ens.fr/~stern/data/St91.ps) is very practical, making minimal assumptions about known plaintext; when that attack was published, in the year 2000, the authors suggest that the attack could be performed in around 2.5 days with an investment on less than $20000. Since then the speeds have probably increased and the costs decreased to some extent. So if it is sufficiently valuable to an attacker to eavesdrop on a particular A5/3 subscriber, it is conceivable that a BBK-style attack based on forcing the reuse of the same key with A5/1 could be worthwhile for that attacker. However, it must be noted that, as well as the cost of A5/1 cryptanalysis, there will be additional cost and complexity involved in picking out and recording the target subscriber's calls, and in deploying the false base station to carry out the practical attack. Setting against this the fact that A5/3 uses only a 64 (or 54) bit key — and of course that other more direct forms of eavesdropping may be possible — it is not clear that this is necessarily the most cost effective route

	for an attacker. **Dynamic cloning:** It does not seem possible with known techniques to break A5/1 in sufficiently "real time" and with sufficiently little known plaintext to carry out a BBK-style dynamic cloning attack. There appears to be a reasonable safety margin here, although we cannot guarantee that cryptanalytic attack techniques may not improve.
A5/2	Extremely weak. There is some slight barrier to eavesdropping provided by the fact that GSM is digital rather than analogue (so you can't eavesdrop just by tuning in a radio receiver); there is also a barrier provided by the subscriber anonymity features in the GSM standard. A5/2 provides no more protection on top of that. And as we all know, it can be broken fast enough to carry out a dynamic cloning attack (although a potentially detectable delay will result).
A5/3	There is no indication at the moment that any attack faster than exhaustive key search is possible.
GEA1 and GEA2	We believe that neither GEA1 nor GEA2 will be any more vulnerable than A5/1, in terms of whether they provide any more of an "Achilles Heel" on which to base either of the types of BBK-style attack. Hence SA3 should base their discussions on the need for key separation mechanisms on the assumption that A5/1 will be the potential weak point once A5/2 is removed.
GEA3	There is no indication at the moment that any attack faster than exhaustive key search is possible.