3GPP TSG SA WG3 Security — S3#31 **S3-030682**
18 - 21 November 2003
Munich, Germany

Title: **LS on request for information on impact on equipment of solutions**
Response to:
Release:
Work Item:

Source: GSMA Security Group working Party
To: SA3
Cc:

Contact Person:
Name: Charles Brookson
Tel. Number: +44 20 7215 3691
E-mail Address: **cbrookson@iee.org**
Comments should be sent to the GSM Association who will correlate replies, anonymously if required: David Maxwell dmaxwell@gsm.org

Attachments: Refer to inputs to SA3 on this topic.

1. Overall Description:

Liaison to Operators and Manufacturers: Request for information

We have looked at the implications of the Vodafone and Orange proposals for special RAND tabled at recent SA3 meetings. These essentially allow a home operator to restrict the set of algorithms (A5 and GEA variants) that a customer's phone may be able to use for encryption. A number of additional (complementary) features have also been identified that may help minimize the impact, and these are described below.

There are various implications to the scheme and issues that we would like comments from:

- Operators, on the impact some of the proposals have on various network components.
- Manufacturers, with the impacts on complexity, timescales (when they can be introduced) and costs on both mobiles and infrastructure (BTS and perhaps the MSC and HLR).

In particular we can expect the impacts on the:

- HLR/AuC,
- BTS and other network elements, e.g. SGSN for GEA, or maybe the BSC and MSC (although the special RAND proposal should not have an impact here).

- ME,
- Signalling within the network (although at present none of the proposals should have an impact on MAP).

2. Actions:

Comments from the Operators, GSMA and manufacturers are invited on the issues below. Some of them are for other approaches to our main special RAND proposal.

- We would like comments as soon as possible, but definitely by the end of 2003.
- Comments should be sent to the GSM Association who will correlate replies, anonymously if required: David Maxwell dmaxwell@gsm.org

Removal of A5/2 from the handset
One proposal is to remove support of A5/2 from new handsets (perhaps alongside the introduction of A5/3). Possibilities are:

- Removal of A5/2 from ALL new handsets;
- Making support of A5/2 optional rather than mandatory — so the manufacturer may choose, or the purchaser may specify, whether or not A5/2 should be supported.

An important question here is what happens when the owner of a handset that does not support A5/2 is a subscriber in, or roams to, a network in which A5/2 is the only available algorithm. Does the network allow unciphered calls? Or will the connection fail? Comments from operators that use A5/2 are particularly invited here.

Wider availability of A5/1
As support for A5/2 in handsets is reduced, it is hoped that A5/1 might be made more widely available to operators. (Of course this is subject to export control regulation.) If A5/1 were available to more operators, would they implement it? How soon? *Of course, the preferred long-term solution is A5/3 and views would be welcome on this as well.*

Increase in the number of authentications
It would be possible to authenticate for every call, and on other occasions (such as Local Area Updates). This has an impact on signalling and loading of various parts of a network, but has the advantage of decreasing the usefulness of getting the key Kc (as it is soon exhausted).

User configurability of the handset
A user should be able to configure which algorithms a handset should (or should not) support. It was thought that it would be a good idea if this were an agreed special command (*# sequence), which could not be reached through a standard menu tree (so that it cannot be easily found, in order not to confuse the uninterested user). Operators could use this for special customers who were concerned, and in case of further developments or weakness.

Infrastructure impact
Support for the special RAND proposal will require (in order to take full advantage of the mechanism) the HLR to have an updateable table of which algorithms are supported within which network. This may be a manual table (derived from roaming agreements), or it may be an automatic table. A manual table will clearly be only as stable as the algorithms in the visited network (for example, if they were changed for network change or in case of load). Comments would be welcome of the feasibility of both approaches.

Note 1: it should be noticed that some protection against man in the middle attacks can be achieved by the special RAND mechanism even without table being available, since no table is needed in order to protect the home network and in order to introduce a full separation between circuit-switched GSM and GPRS.

Note 2: there may be a danger that an operator turns off encryption for a short time, without much warning (perhaps to monitor traffic on an interface in the presence of some technical problems). If the special RAND mechanism is used to require the use of a specific algorithm, then this could lead to call failures. However, if the mechanism is used merely to *disallow* the use of A5/2, for instance, without excluding the use of A5/0, then calls will not fail as long as the visited network supports unciphered calls.

Updates to BTSs, BSCs and MSCs
Various alternatives to the special RAND mechanism have been suggested, which are arguably “cleaner”, and give better protection against man in the middle attacks. However, these mechanisms require changes to the visited network as well as to the home network and the mobile. Indeed, some require ALL possible visited networks — i.e. all GSM operators — to implement the new functionality. Updates may be required to BTSs, BSCs or MSCs, depending on precisely which mechanism is selected.

Comments from operators are invited about the costs of such developments. For example, if networks update their BSC software to the “latest version” every six months anyway, then incorporating new software may not imply a substantial cost. On the other hand, if operators have to upgrade all their BTSs just for this purpose, then the cost may be substantial. How often are MSCs, BSCs and BTSs upgraded?

Network timing
{To be added if required, this solution is still under review.}

3. Date of Next WG Meetings:

Replies are requested by end 2003. Regular meetings are held by conference calls.