SMG 10 meeting / 3GPP TSG SA WG3 Security — S3#11 **S3-000106**

22-24 February, 2000

Mainz, Germany

SMG 10 meeting

February 22-24, 2000
Mainz

GPRS encryption

Input paper for discussion

Source: Telia

1 Background.

SMG #31 Feb14-17 decided that our CR 03.20 on GPRS encryption should be transferred back to SMG 10 for further consideration and completion. Also the CRs on 02.07, 22.101 and 22.060 treated by S1 on GPRS encryption have been postponed.

SMG 10 has now the possibility to tidy up the complete set of CRs relating to GPRS encryption. The set of CRs should then be approved together at either SMG#31 bis or at SA#7. Next ordinary SMG #32 is in June, which seems too late, email approval may be a further possibility. (If it is to 3G SA or SMG to approve is a matter of the outcome of SMG future role?)

2. The issues which are difficult to combine.

Mainly three issues have been discussed relating to GPRS encryption:

a) GPRS should have mandatory encryption as protection against false base stations/SGSN. (This was introduced by SMG 10 in 03.20 already in Oct 1997, but seems later on to have been modified to less stringent writing without SMG 10 awareness!?)

b) Some operators claim that a plain text mode for GPRS terminals is essential for testing and tracing purposes.

c) Some manufacturers claim that export to some countries would be hampered if encryption is mandatory for GPRS.

3. The algorithm choice

Another issue which is still open is the time scale for introducing GEA2. Mandatory in terminals from what date? Should the phase out date for GEA1 be the same date?
It should be clear that encipherment capability is mandatory to support from the start (i.e. at least GEA1).

4. A way forward

From a strict security point of view we would like to mandate networks and terminals to cipher, which leads to requirement on explicit control on both sides that ciphering gets activated and is continued. Of course it also requires that at least one common algorithm is supported between MS and SGSN. The natural choice would be GEA1 from the start and GEA 2 from a certain date

this year (2000) which we fix asap. We can wait with setting date for dismissing GEA1 as mandatory though.

However, to allow testing and certain networks to have traffic in plain text mode would require the option of 'no encryption' to be supported both by SGSN and MS.

To allow a network to do this could possibly be accepted and is anyway hard to control. One has to assume that a responsible operator would only allow it for limited testing and fault searching purposes either in a network not open for general traffic or only to certain terminals under his own control. And a network which by national policy is not allowing encryption is anyway impossible to control.

To allow a plain text mode for terminals is harder as the encryption is mainly a feature for protecting the user and his traffic, e.g. against FBS attacks and even given ciphering indicators the effect on overall security would be increased uncertainty. And if networks can not be trusted to always have encryption on the onus to control this lies with the terminals.

However, one way to allow this, which seems to give a sufficient protection, is to have all MS set for mandatory encryption by default and from factory. Only by user interaction via user menu could the user set the terminal in a "Plain Text Test mode" (PTT mode for short). The PTT mode setting should be accompanied by warnings and only be possible under user password control. It would allow plain text traffic as well as the normal ciphered traffic. This would allow operators easily to have plain text traffic to certain test terminals and in principle also some operators to run their networks without encryption by instructing their users on how to set their terminals in PTT mode. Also roamers from normal encrypting networks could then, by their own choice, set their terminals in PTT mode to allow plain text traffic (rather than no traffic at all) when visiting these networks.

5. Results

- We would still have very good protection against false base station attacks, in most parts of the world
- The (old GSM) problem of subscribers being uncertain if the network they are using is ciphering or not would go away, leading to increased user confidence.
- The testing problem would be solved by using standard MS, set in PTT Mode and a special test mode on the SGSN (possibly needed to be targeted to the special test terminals?).
- Some national networks which are not allowed to have encryption will still be able to buy standard equipment.

6 Where to set the PTT mode?

In principle the PTT mode could be set in the ME or in the SIM card.

Some smaller advantages seem to make the SIM the preferred choice:

- It is more natural to control the user access to the SIM and thus to have it combined with access control to set PTT mode

- The user may acquire a used ME and may forget to check or be unable to change back from PTT mode. (But for users to acquire a “used” SIM is not a natural behavior, the SIM is more strongly connected to the user and his preferences than the ME).
- For testing, special test SIMs could be used which already have the PTT mode set and would immediately be recognized by the network as such.
- The non-encrypting operators’ users could get the PTT mode directly in their SIMs as issued by their operators, no need for user settings. (is this an advantage?)