**SMG 10 meeting / 3GPP TSG SA WG3 Security — S3#11** **S3-000205**

**22-24 February, 2000**

**Mainz, Germany**

---

**Source: SMG10/SA WG3**

**Subject: Discussion paper on GPRS Encryption**

This paper's objective is to describe the functions necessary to protect GPRS from hijacking attacks and provide protection from false base station attacks in networks that activate ciphering (which should be a vast majority of operators) and to propose a schedule for the introduction of these functions in the GPRS specifications. Also we try to identify which specifications and other SMG groups are concerned by the proposed changes.

The solution identified to prevent these attacks is based on Tdoc S3-000106 and Tdoc S3-000137. GPRS encryption shall not be made mandatory, but the proposal is that encryption should be the normal mode of operation of GPRS networks and that the GSM Association strongly recommends its members to activate ciphering.
To ensure this, all terminals shall support at least one GPRS encryption algorithm (GEA1 in a first phase and GEA2 as soon as possible). Also, to counter the false base station attack, it shall be possible for terminals to reject non ciphered calls. By default, terminals shall reject non ciphered calls but the user can configure the terminal to accept non ciphered calls (and optionally, the network if this function is controlled in the USIM).

So the following points have to been either made clear or introduced in the GPRS specifications:

- Mandatory support of a GPRS algorithm in terminals
- Mandatory support of ciphering indicator in terminals
- Rejection of non ciphered calls by terminals, and possibility to de-activate this feature

**Introduction of GEA2:**

There is also the issue of the introduction of GEA2 in GPRS networks. It is unfortunately too late to swap out GEA1 completely, therefore scenarios to ensure the proper migration towards GEA2 must be studied.

In a first phase, terminals shall support GEA1 as an encryption algorithm. As soon as possible, terminals shall support GEA1 and GEA2 (terminals have to support both in case the user is roaming in a GPRS network that has SGSNs supporting only GEA1). SGSN shall as fast as possible support both GEA1 and GEA2 and hopefully, networks can switch to using mostly GEA2.

**Opened issues to be discussed**

Whether the configuration of the rejection of non ciphered calls is to be placed in the terminal or the SIM has to be decided. As pointed out in S3-000106, there are advantages and disadvantages to either choice:

- Configuration in the SIM
  - Advantages: it would be fitting to have that parameter set in the SIM since it is an operator specific parameter. Also, having it in the SIM would allow operators to modify it through the radio interface which might be useful.
  - Disadvantages: GPRS terminals with old SIMs inserted will not support the feature.
- Configuration in the terminal
  - Advantages: it might be simpler and faster to achieve since it will not impact the SIM. Also it avoids the problem of having to change the SIM for GPRS suscribers.

Proposed solution:

It is suggested that the acceptation of non ciphered calls can be done both via the SIM and the ME. The mechanism would be the following:

- The ME checks if ciphering is on, and if not, the connection shall be released
- The rejection of non ciphered connections may be disabled by the SIM if this option is supported by the SIM
- The rejection of non ciphered connections may be disabled by the user through a menu, either via the SIM if the SIM supports this option, either directly in the ME
- The SIM setting when active would override the ME setting.
- By default, both the ME and the SIM shall be configured to reject non ciphered connections

**Proposed schedule**

**Release 97**

Since release 97 cannot be heavily modified, we mainly propose to clarify the GPRS specifications to ensure that support for encryption and ciphering indicator is present in the terminals.

**Mandatory support for GEA1 in terminals**
Specs affected: 02.07 (terminal requirements), 11.10 (terminal tests)
Groups affected: S1, T1

**Support of ciphering indicator in terminals**
Specs affected: 02.07 (terminal requirements), 11.10 (terminal tests)
Groups affected: S1, T1

**Release 98**

R98 should introduce support for the rejection of non ciphered called in the terminal and SIM.

Release 98 should be the beginning of migration from GEA1 to GEA2. It would be best that equipment (terminals and SGSN) support both GEA1 and GEA2, but since it is unclear whether this can be achieved, support of GEA1 is mandatory and support of GEA2 is optional.

**Support of GEA1 or GEA1 and GEA2 in terminals and SGSN**
Specs affected: 02.07 (terminal requirements), 11.10 (terminal tests)
Groups affected: S1, T1

**Setting for rejection of non ciphered calls in terminals/SIM**
Specs affected: 02.07 (same as cipher indicator)? 04.08? 04.64? 04.65?
Groups affected: S1, N1, T2, T3

**Release 99**

Release 99 GPRS terminals and SGSN shall support GEA2 which will ensure that GEA1 will eventually be phased out of GPRS. Therefore all R99 terminals and SGSN type approved after 31/12/02 shall support both GEA1 and GEA2.

**Mandatory support of GEA1 and GEA2 in terminals**
Specs affected: 02.07 (terminal requirements), 11.10 (terminal tests), 22.101, 22.060
Groups affected: S1, T1

**Mandatory support for both GEA1 and GEA2 in SGSN**
Specs affected: 04.08?
Groups affected: N1?