3GPP TSG SA WG3 Security — S3#11 **S3-000192**

22-24 February, 2000

Mainz, Germany

Source:	**France Telecom**
Title:	**Proposed LS to N1 about rejection of non ciphered calls for GPRS**
Document for:	**Approval**
Agenda Item:	**6.1**

Source:	**SMG10**
To:	**SMG3/3GPP N1**
Cc:	**3GPP T2, SMG9**
Title:	**Introduction of rejection of non ciphered connections in GPRS**

SMG10 has identified serious threats upon GPRS systems when ciphering is not activated that can lead to frauds and/or false base station attacks. Encryption control by the network is not deemed sufficient to provide good protection against these attacks.

Since it has proven problematic to make ciphering mandatory in GPRS, SMG10 has agreed that a mechanism that would allow terminals to reject non ciphered connections is required. Such a mechanism would ensure that non ciphered connections cannot be established without the user being aware of it and would provide protection against false base stations attacks. It should be noted that ciphered connections are expected to be the general case for GPRS networks and that non ciphered connections should happen in special cases only (tests phases and maybe in some countries that do not allow the use of encryption).

Such a mechanism would work in the following way:

- By default, all terminals shall reject non ciphered connections
- It shall be possible for the user to accept non ciphered connections by changing a setting in the MS, either in the SIM or the ME.

SMG10 suggests that both the SIM and the ME contains a parameter to accept or reject non ciphered connections, and that the SIM parameter, if present, shall override the ME parameter. The exact way to control the rejection of non ciphered connections in the MS remains to be completed by SMG10.

SMG10 wants to stress the importance of such a mechanism and that it would be highly desirable to introduce it as soon as possible in GPRS systems.

SMG10 therefore kindly asks N1, T2 and SMG9 to consider the modifications necessary for the introduction of this mechanism and to identify the specifications that require changes to specify this mechanism.