TSG-SA WG3 (Security) meeting #12
Stockholm, Sweden, 11-14 April 2000

S3-000306

LIAISON STATEMENT

From: SA3

To: SMG, CN1/SMG3

Subject: GPRS ciphering

Rejection of non-ciphered packet connections

SA3/SMG10 thanks CN1/SMG3 for their LS on the rejection of non-ciphered packet connections (N1-000539, S3-000219). SA3/SMG10 regrets that CN1/SMG3 sees no chance to include this important feature in Release 99. Non-ciphered packet connections are insecure and users and their home environments should have the ability to protect themselves against the risks. SA3/SMG10 will continue work on this work item for inclusion in **Release 00**.

Mandatory ciphering indicator

SA3/SMG10 wants to draw to the attention of CN1/SMG3 that **GSM 02.09 mandates the presence of a ciphering indicator** in the ME, and that GSM 03.20 mandates that, when a ciphered connection is established, non-ciphered frames are discarded by the ME and that, once a ciphered connection is established, it is not acceptable to the ME to turn it off. This helps to alleviate the extent of the problem arising from the lack of the ability to reject non-ciphered connections.

Support for multiple GPRS ciphering algorithms in GSM 04.08/TS 24.008

SA3/SMG10 has reviewed GSM 04.08/TS 24.008 and has found that the ME does not have the ability to signal to the SGSN information about its GPRS ciphering capabilities other than whether it supports GEA/1. **The ME must have the ability to signal its capabilities on 7 GPRS ciphering algorithms.** SA3/SMG10 suggests that the MS network capability information element be extended by a second octet and that part of the additional bits are used to indicate the capability to support GEA/2, …, GEA/7. SA3/SMG10/SMG10 believes changes should be carried out at least starting **from Release 98**, as we propose – and hope to be endorsed – that support for GEA/2 is optional in Release 98 and mandatory for Release 99 from end of 2002 onwards.

We urge CN1/SMG3 to resolve this issue.

Optional/mandatory GPRS ciphering

SA3/SMG10 have reviewed their work on mandatory GPRS encryption in the light of the comments provided by the SMG plenary. SA3/SMG10 have revisited the topic and regrets that mandatory GPRS encryption is not achievable at this stage. **SA3/SMG10 has agreed on a CR against GSM 33.20 clarifying that non-ciphered connections can be established if the network so wishes.** SA3/SMG10 also added a line saying that if the ME signals a non-compliant set of supported algorithms (as defined in GSM 02.09) the network shall release the connection. SA3/SMG10 confirms that mandatory GPRS ciphering is not a part of Release 99. SA3/SMG10 however continues the work on this work item for **Release 00**.