3GPP TSG SA WG3 Security — S3#14 **S3-000418**

2-4 August, 2000

Oslo, Norway

Source: **T WG2**

Title: **E-mail on Rejection of non-ciphered connections**

Document for: **Discussion**

Agenda Item:

Transcript of an e-mail which had been forwarded to SMG10/SA WG3 from Kevin Holley on Rejection of non-ciphered connections (informal liaison statement).

Dear David,

T2 had a brief discussion on the attached LS and thought that an email might work better than a formal LS to SMG10.

The modifications needed for this would concern the addition of AT commands to change the setting of accepting or not accepting non-ciphered connections. This would enable the changes to be made to these settings for mobiles with no MMI (e.g. PC-card implementation). T2 has so far had no

input on these items and therefore has not progressed the work on this.

This is not a big matter, however interested companies are invited to make the input.

Please confirm that you received these comments OK.

Best Regards,

Kevin Holley

3GPP TSG-T2 #9 / ETSI SMG4 Utrecht, NETHERLANDS 15 - 19 May 2000 T2-000170

3GPP TSG SA WG3 Security - S3#11 S3-000206

22-24 February, 2000

Mainz, Germany

From: SMG10

To: SMG3 / 3GPP CN WG1

CC: 3GPP T WG2, SMG9

Title: Introduction of rejection of non ciphered calls for 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.

Attachment: TD S3-000205: "Discussion paper for GPRS encryption"

> --

> Kevin Holley

> 3GPP TSG T Vice Chairman

3GPP TSG T2 & SMG4 Chairman

> BT Adastral Park

> Tel: +44 1473 605604

> Fax: +44 1473 619027

> Mobile: +44 7802 220811

>

>