3GPP TSG SA WG3 Security — S3#28   **S3-030271**
6 - 9 May 2003
Berlin, Germany

Title:	**DRAFT Security issues regarding multiple PDP contexts in GPRS**

Source:	**SA3**
To:	**SA2**
Cc:	**CN4**

Reply to:	**S2-031589**

Contact Person:
    Name: **Peter Howard, Vodafone**
    Tel. Number: +44 1635 676206
    E-mail Address: peter.howard@vodafone.com

Attachments:	None

SA3 has considered the LS from SA2 (S2-031589) which asks SA3 to clarify the nature of the security threats associated with multiple simultaneous PDP contexts in GPRS.

In the LS SA2 made the following comment:

"Specifically, there were questions on whether it was worth blocking multiple simultaneous PDP contexts when similar "problems" could be caused by successive PDP contexts with eg data being downloaded from an intranet, stored in the mobile, and then uploaded to the internet."

In response to this comment, SA3 believes that in general real-time access to a private network (e.g. corporate LAN) from a public network (e.g. the Internet) allows more powerful attacks to be performed compared to the case where real-time access is not possible. Furthermore, SA3 believes that real-time attacks could make use of existing software that is legitimately present on the terminal, whereas some attacks which do not involve real-time access would require the attacker to plant trojan software on the terminal. Attacks which do not involve real-time access are therefore considered to be both more difficult to mount because they require more control over the user's terminal and easier to detect. For these reasons SA3 consider it worthwhile to block simultaneous PDP contexts even if successive PDP contexts are still allowed providing that the mechanism to block simultaneous PDP contexts for particular combinations of APNs is cost effective.

Actions

None.

Next SA3 Meetings

SA3 meeting #29   15th – 18th July 2003   San Francisco, CA, USA

SA3 meeting #30   7th - 10th October 2003   TBD