3GPP TSG-SA WG2 meeting #37 **Tdoc S2-040468**
Innsbruck, 12th – 16th January 2004

Title: **Reply to LS (S2-030027/S3LI03_124r1) on 3GPP WLAN interworking Lawful Interception Requirements**

Release: **6**

Source: **SA2**

To: **SA3 LI**

Cc: **SA3**

Contact Person:
Name: **Mark Watson**
E-mail Address: **mwatson@nortelnetworks.com**

Attachments: None

1 Overall Description

SA2 thanks SA3 Lawful Interception group for their LS (S2-040027/S3LI03_124r1) on Lawful Interception requirements for 3GPP WLAN Interworking.

During the discussion of this liaison a number of questions were raised on which SA2 would like to receive clarification from SA3 LI experts.

SA2's current architecture for Scenario 3 (end-to-end tunnelling) involves a secure tunnel being established between the UE and the Packet Data Gateway. User data within this tunnel will be encrypted by the UE and the PDG. In the case that the PDG is within the Home Network, therefore, no encryption/decryption is applied by the Visited Network.

SA2's questions are:

- In this scenario, is there still a requirement for the VPLMN to provide unencrypted data for Lawful Interception purposes ?
- If yes,
  - is it necessary for the VPLMN to provide actual unencrypted data, or would it be sufficient to supply only the keys/algorithm type along with the encrypted data stream

    (Note that VPLMN decryption of the data implies a requirement for the UE and PDG to restrict themselves to decryption algorithms supported by the VPLMN).
  - SA2 was unclear why the situation for the VPLMN is then different from the situation for an Internet Service Provider which provides IP transport services between UE/WLAN and the HPLMN. SA2 notes that the service provided by the VPLMN in this case (and specified in the various business/roaming agreements between WLAN, VPLMN and HPLMN) is essentially equivalent to a simple Internet transport service provided by an ISP.

SA2 would like to note that from their perspective the keys/algorithm used to encrypt/decrypt the data could be provided by the HPLMN to the VPLMN for LI purposes. However, the exact details of how this might be done and when it should be done (e.g. every time for every user or only sometimes for some users) are a matter for SA3 LI.

SA2 further notes that in the case where the PDG is provided by the VPLMN, then the VPLMN does provide encryption/decryption of the user data (at the PDG). SA2 does not see any issues with providing the LI functionality described in SA3 LI group's liaison in this case.

2 Actions

To SA3 LI Group:

ACTION: **Provide clarification to SA2 on the questions above.**

3 Date of Next 3GPP SA2 meetings

TSG SA WG2#38	16 – 20 February 2004	Atlanta, US
TSG SA WG2#39	19 - 23 April 2004	TBD, China