3GPP TSG SA WG3 Security — S3#32
09 - 13 February 2004
Edinburgh, Scotland, UK

S3-040138

3GPP TSG SA WG3 LI Meeting 04/01
Miami, US, 27 – 29 January 2004

S3LI04_042r1

Title:	**Reply to LS (S2-040468) on 3GPP WLAN interworking Lawful Interception Requirements**
Release:	**6**

Source:	**SA3 LI**
To:	**SA2, SA3**
Cc:	

Contact Person:
    Name: **Brye Bonner**
    E-mail Address: **brye.bonner@motorola.com**

Attachments: None

1 Overall Description

SA3 LI thanks SA2 group for their LS (S2-040468) on Lawful Interception requirements for 3GPP WLAN Interworking.

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 ?

S3 LI answer would be, if the VPLMN is not involved in the encryption, according to 3GPP TS 33.106, there is no requirement for the VPLMN to decrypt the data (or provide the keys) encrypted by UE and HPLMN PDG.

S3 LI hopes that the above clarifies the matter. Please provide further questions as necessary.

2 Actions

None

3 Date of Next 3GPP SA3 LI meetings

TSG SA WG3 LI #04/02	14-16 April 2004	Italy
TSG SA WG3 LI #04/03	12-14 October 2004	USA