

**3GPP TSG SA WG3-LI**  
**18-20 November 2003**  
**London, England**

**S3LI03\_124r1**

---

**Title:** LS on 3GPP WLAN interworking Lawful Interception Requirements

**Release:** Release 6

**Source:** SA3 LI

**To:** SA3,SA2

**Cc:**

**Contact Person:**

**Name:** Alex Leadbeater

**E-mail Address:** [alex.leadbeater@bt.com](mailto:alex.leadbeater@bt.com)

**Attachments:** None

---

## **1 Overall Description**

3GPP TSG SA WG3-LI thanks SA3 for their contributions S3-030557/S3LI03\_115 ( UE-Initiated Tunnelling with IKEv2) and S3-030550/S3LI03\_116 (Evaluation of alternatives for secure set-up of UE initiated tunnels). SA3 LI are still in the process of considering detailed LI requirements for WLAN interworking. However in the interim, SA3 LI would like to inform SA3 and SA2 of a number of initial concerns and requirements relating to 3GPP WLAN interworking scenarios 2 and 3.

For scenario 2, SA3-LI did not identify any specific LI issues that are not addressed by existing 3GPP LI mechanisms.

In the case of scenario 3, there is an underlying LI requirement for the 3GPP network operator to be able to remove any encryption applied by the network operator to traffic passing through their network for the purposes of Lawful Interception. Where the WLAN and the HPLMN are in the same country or when the PDG is in the visited 3GPP network, SA3 LI did not identify any major LI issues resulting from S3-030550/557.

Where the WLAN and the PDG are located in different countries, from an S3 LI prospective, any arrangement in which the visited network cannot deliver unencrypted traffic (or provide the keys), may raise serious regulatory issues.

SA3 LI acknowledge that 3GPP WLAN subscribers may use tools such as PGP phone to encrypt their traffic end to end, which the visited or home network cannot decrypt. However, in this scenario the way in which encryption is applied is outside the scope of 3GPP standardisation, since there are no commercial or roaming agreements directly involving the visited network. In scenario 3 where the PDG and WLAN are in different countries, then there are formal commercial and roaming agreements in place, which may require the visited network to deliver unencrypted traffic (or provide the keys) for the purposes of lawful intercept.

SA3 LI accept that work on 3GPP WLAN interworking standardisation is still on going. SA3 LI would welcome further details from SA2 and SA3 as and when their specifications develop further.

## **2 Actions**

**To SA3 Group:-**

**ACTION:** SA3 LI request that SA3 take SA3 LI's comments into account when progressing their work on 3GPP WLAN interworking security.

**To SA2 Group:-**

**ACTION:** SA3 LI request that SA2 take SA3 LI's comments into account when further developing their 3GPP WLAN architecture specifications.

## **3 Date of Next 3GPP SA3 LI Meetings**

3GPPSA3-LI#12	27-29 January 2004	USA. (Location TBC)
3GPPSA3-LI#13	14-16 April 2004	Europe (Location TBC)