3GPP TSG SA WG3 Security — S3#34 **S3-040459**
July 6 - 9, 2004
Acapulco, Mexico

3GPP TSG-SA WG2 Meeting #40 **Tdoc S2-042316**
Sophia-Antipolis, France, 17th – 21th May 2004

Title:	**Clarification on Addresses used for Tunnel Establishment**
Response to:	-
Release:	Rel 6
Work Item:	Interworking WLAN
Source:	SA2
To:	SA3
Cc:	-

Contact Person:
Name: **Rainer Liebhart, Siemens**
Tel. Number: **+49 89 63675210**
E-mail Address: rainer.liebhart@siemens.com

1. Overall Description:

To access PS services like IMS a WLAN UE has to establish first a secure tunnel to the PDG in the mobile core network providing the service. The tunnel endpoint IP address is determined by the WLAN UE resolving the selected W-APN FQDN using standard DNS mechanisms. The WLAN UE obtains its local IP address from the WLAN AN or the VPLMN. In principle the WLAN UE can associate to a WLAN AN that supports IPv4 or IPv6 addresses. On the other hand, the W-APN DNS resolution procedure may return also an IPv4 or IPv6 address. It is not clear to SA2 whether the WLAN UE is able to establish a secure tunnel to the PDG, if the tunnel endpoints at the WLAN UE and PDG use IP addresses of different IP versions.

2. Actions:

SA2 kindly asks whether SA3 sees any problems from a security point of view to establish a secure tunnel between the WLAN UE and the PDG, if the WLAN UE has obtained a local address with an IP version different from that of the tunnel endpoint at the PDG, e.g. by using mechanisms like IP-in-IP encapsulation.

3. Date of Next TSG SA WG 2 Meetings:

TSG-SA2 Meeting #41	16-20 August 2004	Montreal, Canada
TSG-SA2 Meeting #42	11-15 October 2004	Sophia-Antipolis, France