3GPP TSG SA WG3 Security — S3#28 **S3-030205**
6 - 9 May 2003
Berlin, Germany

3GPP TSG-SA WG2 meeting #31 Tdoc S2-031510
Seoul, Korea, 7th – 11th April 2003

Title: Security in WLAN and 3G interworking
Response to: S2-031120/S3-030167
Release: Rel-6
Work Item: WLAN

Source: SA2
To: SA3
Cc:

Contact Person:
Name: **Mark Grayson**
Tel. Number: +33.6.19.98.40.99
E-mail Address: mgrayson@cisco.com

Attachments: None.

1. Introduction:

SA2 thanks SA3 for the LS S3-030167 addressing security in WLAN and 3G inter-working.

In terms of the architectural requirements, SA2 would like to confirm that the requirements impacting 802.11i/WPA discussions include:

- The support of mutual authentication
- The support of per-user per-session key exchanges
- Re-keying techniques which may be required to overcome inherent weaknesses of a deployed encryption algorithm.

As well as protecting the WLAN air interface, the above techniques can be used to build support for non-repudiation of WLAN accounting records.

Accordingly, it is the understanding of SA2 that the above requirements can be fulfilled using either IEEE 802.11i or the standards based WPA.

From an SA2 perspective, the architectural impacts of defining WPA due to R'6 deadline issues are limited to keying issues. In particular, it is envisaged that the length of the key distributed during mutual authentication and key exchange shall be sufficient to accommodate AES requirements and that the AAA Client shall be responsible for any necessary truncation. SA2 notes that mandating AES may place additional requirements on the WLAN Access Network.

SA2 agrees with SA3 that protection should be provided for WLAN authentication data and keying material on the Wr interface. SA2 notes that the protection techniques need to accommodate RADIUS to Diameter Interworking, e.g., guidelines for EAP message transport mandate the use the RADIUS Message Authenticator Attribute whereas Diameter prohibits the transport of this attribute. SA2 is currently analysing issues around Diameter to RADIUS interworking.

Finally, previous discussion has highlighted that HIPERLAN2/HiSWAN has defined the use of EAP using functionality termed EAP over HIPERLAN (EAPoH). SA2 is awaiting further contributions addressing such alternative radio LAN technologies.

2. Actions:

To SA3 group.

- **ACTION:** Since AES support may require hardware changes to elements in the WLAN Access Network, SA3 are asked to confirm that the WPA defined encryption meets the security requirements for WLAN-3GPP inter-working.

- **ACTION:** SA3 are requested to comment on any security implications of RADIUS to Diameter inter-working

3. Date of Next SA2 Meetings:

Meeting	Date	Location	Host
SA2 WLAN Ad Hoc	**28-30 April, 2002**	**Oslo, Norway**	**Telnor**
SA2#32	**12-16 May , 2002**	**San Diego, USA**	