3GPP TSG SA WG3 Security — S3#26 **S3-020694**
19- 22 November 2002
Oxford, UK

Title:	**Reply LS on: "3GPP System – WLAN Interworking"**
Source:	**SA3**
To:	**SA2**
Cc:	
Response to:	**LS S2-023122 on 3GPP – WLAN interworking**

Contact Person:
Name: **Sébastien Nguyen Ngoc (Orange)**
Tel. Number: **+33.1.45.29.47.31**
E-mail Address: **sebastien.nguyenngoc@rd.francetelecom.com**

Attachments: **None**

SA3 thanks SA2 for their liaison statement on 3GPP System – WLAN interworking. SA3 has examined issues raised by SA2 and provides the following answers.

1. Security requirements

SA3 has taken into account SA2 request to have all security requirements located in TS 33.234. In a similar way, SA3 has removed all non security related requirements from TS 33.234 since these are addressed in TS 23.234.

2. Temporary identities

SA3 has examined the issue of temporary identities in the case of 3GPP System – WLAN interworking. SA3 decision was to endorse as a working assumption a mechanism based on encryption of the IMSI. This mechanism fills SA2 requirement of having a stateless AAA server and no user related information needs to be stored in the AAA server. SA3 however outlines that it does not provide with enhanced identity confidentiality compared to the 3GPP TMSI mechanism, because there is a need for a recovery mechanism that allows the network to request the IMSI from the UE.

SA3 provides the following answers to some questions asked in the liaison statement:

- *WLAN authentication necessitates the use of a temporary identifier, which needs to be stored somewhere in the terminal; however in pre-R6 implementations, it is not possible to store it within pre-R6 (U)SIMs. SA2 wonders if it raises security issues;*

SA3 sees no major security issues with storing the temporary identifier in the terminal. In the case where a user inserts his SIM/USIM in another terminal, the recovery procedure will be used and the IMSI will be sent in clear.

- *How to keep the AAA Server stateless by e.g. including the IMSI encrypted within pseudonym ?*

The mechanism chosen as a working assumption by SA3 ensures that the AAA server is stateless and needs not to store user related information.

- *Is it acceptable security-wise that the network can request the IMSI from the UE at any time?*

Recovery mechanism requires for the network to be able to request the IMSI from the UE. Whether this request is transparent or not to the user is still under consideration.

3. Alternative mechanism for identity protection

SA3 is currently reviewing PEAP as a potential method to protect the authentication mechanism for 3GPP System – WLAN interworking. In the case PEAP was chosen by SA3, it would provide a different solution to identity protection, and SA3 would reconsider their working assumption of using temporary identities.

4. Actions:

To SA2 group

ACTION: None.

5. Next SA3 Meeting:

Meeting	Date	Location	Host
SA3#27	**25-28 Feb 2003**	**Sophia Antipolis, France**	**ETSI**