3GPP TSG SA WG3 Security ó SA3#35 **S3-040839**

October 5-8, 2004, St Paul's Bay, Malta

Title:	**Requirements To be Realized in SAP (SIM Access Profile) when Bluetooth is used as Local Interface for Authentication of Peripheral Devices**
Source:	3GPP SA3
To:	Bluetooth Architecture Review Board (BARB), Bluetooth CAR group and Bluetooth Security Expert Group
CC	
Contact Person:	Dr. Raziq Yaqub (Toshiba America Research Inc.)
	Tel. Number: +1-732-699-2421
	ryaqub@tari.toshiba.com

1. Introduction

3GPP SA3 Working Group is developing the security architecture for interworking of 3GPP System with WLANs that is documented in technical specification TS 33.234 (Latest version attached herewith).

This specification also covers a WLAN-UE functional split scenario under which several peripheral devices may communicate to (U)SIM over local interfaces (e.g. Bluetooth, IR or serial cable). Such a split WLAN-UE will be capable of accessing both WLAN and 3GPP UMTS/GSM systems simultaneously.

As a brief background, WLAN-UE functional split implies split of User Equipment into TE (e.g. a laptop with a WLAN card) and a UE (a GSM/UMTS mobile phone equipped with a UICC containing a SIM or USIM applications). The SIM or USIM is required to authenticate WLAN UE using facilities and techniques provided by 3GPP networks. The authentication and key establishment protocol used for this access is either EAP-SIM or EAP-AKA.

To realize the above noted scenario, SA3 has come-up with some requirements. We feel that if these requirements are fulfilled by introducing a new profile, the use scenario can be realized. It is therefore requested to start work on a new version of the SIM Access Profile, realizing the requirements listed below:

2. Functional Requirements when Bluetooth is used for the Local Link.

With the SIM Access Profile, Bluetooth SIG specified functions which meet some of the requirements for Security Reuse. However, some requirements shall be added to the current SIM Access Profile specification to provide missing functionality and security level for Reuse:

1. The server shall allow itself and one additional device to access the card concurrently when the secure link is established and the external device has been authenticated.

2. Access to SIM, USIM, and ISIM shall be possible.

3. Security Requirements for Communication over local interface via Bluetooth link

1. The local interface shall provide replay protection. The preferred means to achieve this is integrity protection, but other means may be sufficient as pointed out in the liaison statement sent earlier under No. S3-040164 on February 2004.

2. The full 16 octet PIN shall be used for pairing and initialisation key establishment

3. Combination keys shall be used for link key generation.

4. The connection shall be terminated and restarted at least once a day to force the use of a new random number in the Bluetooth ciphering process to prevent key stream repeats

5. The use of a Separate Bluetooth interface/software stack for the local link that cannot be placed in discoverable mode by the user once the pairing process is complete may be considered for high security applications.

6. Only Bluetooth Version 1.2 shall be used which provides protection against interference from the WLAN interface in the same band.

7. Deliberate denial of service attacks on the Bluetooth shall be minimised by reserving at least 20 channels for local link communication.

8. Mandatory authentication and encryption at the link layer (MODE 3 Security) is imposed.

3. Conclusion

SA3 kindly asks Bluetooth SIG to realise these requirements in the new SIM Access Profile. These requirements will provision a new usage model under which a split WLAN UE will become capable of accessing both WLAN and 3GPP systems simultaneously.

SA3 is looking forward to future cooperation with Bluetooth on this issue.

4. Actions to Bluetooth CWG

1. To specify and realise the above noted requirements by defining a new SIM Access Profile or new serial Access Profile.

5. Date of Next 3GPP WG-SA3 Meetings:

Meeting	Date	Location	Host
S3#36	23-26 November 2004	Shenzhen, China	HuaWei Technologies
S3#37	21-25 February 2005	Sophia Antipolis	ETSI
S3#38	TBC	TBC	TBC
S3#39	Summer 2005	San Diego	Qualcomm (TBC)