Technical Specification Group Services and System Aspects **TSGS#20(03)0~~227~~341**
Meeting #20, Hämeenlinna, Finland
09-12 June 2003

3GPP TSG SA WG3 Security — SA3#28 **S3-030307**
6 - 9 May 2003
Berlin, Germany

Title: **WID for Feasibility Study on**
(U)SIM Security Reuse by Peripheral Devices on Local Interfaces

Source: **Toshiba, Intel, T-Mobile, Nokia**
Agenda item: **7.16 User Equipment Functionality Split**
Document for: **Discussion/Decision**

Work Item Description

Title: **(U)SIM Security Reuse by Peripheral Devices on Local Interfaces**

1. 3GPP Work Area

	Radio Access
X	Core Network
	Services
X	Terminals

2. Linked work items

There are no work items directly linked to this WI. However, the following work items are examples that can benefit from the feasibility study.

WLAN interworking security ~~WID~~
~~UE Management~~
~~User Equipment Functionality Split,~~
Subscription Management.

3. Justification

There is a possibility of alternative peripheral devices on local interfaces to user equipment. An existing example is WLAN, and others such as Bluetooth are a distinct possibility. For these diverse usage models the potential security threats and issues need to be evaluated and appropriate security requirements may need to be specified to counteract any potential threats. It is important that the security on these interfaces is under 3GPP control. As an example ~~The~~ the 3G-WLAN interworking requirements specified in TR 22.934 v6.1.0 requires the ability for a SIM or USIM to be used for providing common access control and charging for WLAN and 3G services using the 3GPP system infrastructure. The current specifications of SIM and USIM in 3GPP assume a one-to-one association between the UICC and the Mobile Equipment (ME) to constitute the User Equipment (UE). While this assumption holds in many situations it does not hold for the following examples, especially in the context of WLAN interworking to 3GPP system. These are also shown generically in the figure 1.

Example 1: SIM inside a GPRS card module (ME1) used for WLAN authentication on a Laptop (ME2). It is also used for GPRS authentication.

Example 2: SIM inside a GSM phone (ME1) used for WLAN authentication on a Laptop (ME3) over a Bluetooth local link (Using the Bluetooth SIG, SIM Access Profile Specification). It is also used for GSM authentication.

~~For these diverse usage models the specific security threats and issues need to be studied and appropriate security requirements need to be specified to counteract the threats.~~ Following are some security related issues:

Issue 1: The U(SIM) authentication process once it is complete, the key setting procedure that takes place assumes further use of the same radio interface, namely GSM, GPRS or 3G. For the case of GPRS the Kc and CKSN are saved on the SIM for the subsequent authentications. For the 3G case, the CK and IK are saved for subsequent authentications also.

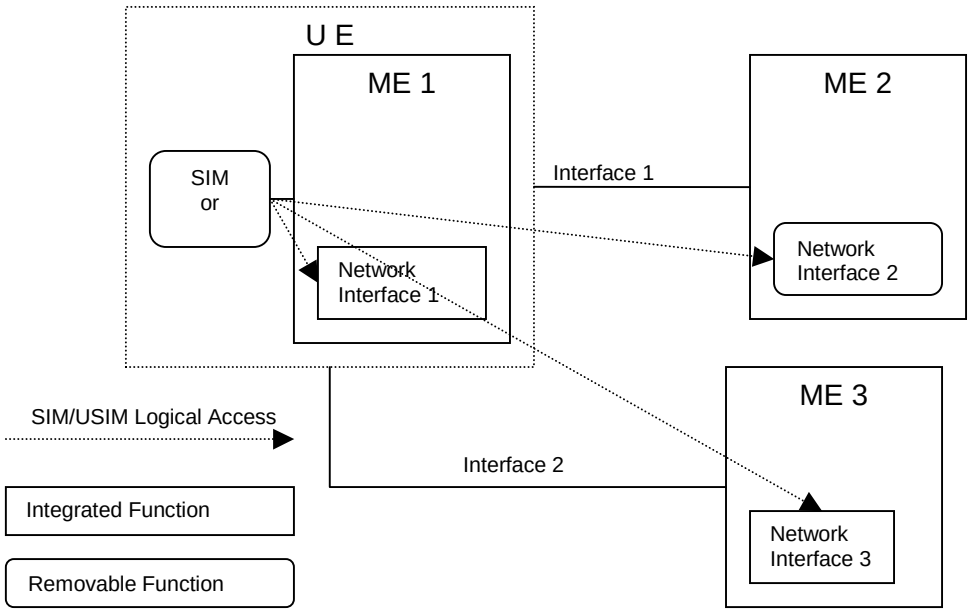

Figure 1: SIM/USIM Re-use Generic Model for Multiple Network Interfaces

Issue 2: The ME that needs to check the presence of the U(SIM) may not be effectively able to do that as is done today for 3GPP terminals, for Example 2 noted above. In the Example 2, the Bluetooth link, if for some reason encounters some interference that prevents SIM presence detection, the WLAN session authenticated using the local link will have to be dropped.

Issue 3: If Pseudonyms are used for Identity privacy as specified in EAP-SIM and EAP-AKA protocols they could be stored on the SIM and USIM respectively or on the ME. This may require additional specification for secure storage.

Issue 4: The SIM and USIM user authentication (PIN entry based) for Example 1 and Example 2 is performed for the native GPRS/GSM or 3GPP system use and also will be needed for the WLAN use for better protection. This may require additional specification and modifications to the U(SIM) or security architecture specifications.

Due to all the above issues, we need this work item to study the issues and develop the additional security requirements for the usage models as considered in Example 1 and 2.

4. Objective

- To study the feasibility of diverse usage models (e.g., as noted above accessing 3GPP system and WLAN simultaneously) including the model with multiple external (wired or wireless) interfaces from a security point of view, and to realize these models without incorporating significant changes to the infrastructure.
- To study the impact on current security specifications for 3GPP, especially with regards to key setting procedures, and USIM sequence number synchronization, UICC presence detection/UICC application presence detection issues and termination of the UICC usage etc.
- To study any additional user authentication requirements (e.g. PINs) when used over local interfaces like Bluetooth, IR or USB.
- To study the impact on having many entities using the same security mechanism and any 3GPP core network elements.
- Conduct a threat analysis related to the proposed new functionality.
- Note: The priority will be requirements and solutions for incorporation into 3GPP-WLAN Interworking security specification TS 33.234.

5. Service Aspects

None Identified.

6. MMI-Aspects

The selection of a U(SIM) for a particular network interface, when multiple choices are available, requires changes to the traditional Man Machine Interface that assumes a single U(SIM).

7. Charging Aspects

Charging maybe affected, and its effects have to be studied. Especially when the same IMSI is used for a single subscriber attaching to the same core network over different network interfaces. However SA5 may have to look at these effects.

8. Security Aspects

This is a Security item.

9. Impacts

Although the end deliverable is a TR, the results, if adopted, could possibly impact the elements in the following table.

Affects:	**UICC apps**	**ME**	**AN**	**CN**	**Others**
Yes	X	X			
No			X		
Don't know				X	X

10. Expected Output and Time scale (to be updated at each plenary)

specifications

Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
TR xxx.yy	Feasibility Study for (U)SIM Security Reuse by Peripheral Devices on Local Interfaces	SA3		SA3 plenary # 29 (July '03)		Agree upon the "Table of Contents" for the Technical Report, conduct threat analysis, and make initial version of the TR available containing technical contents on main parts.
				SA3 ad-hoc (Sept.'03)		. Make 1st version of full TR ready for submission to SA plenary in Sept. '03, for information
				SA Plenary (Sept. '03)		Present 1st version of TR for information
				SA3 plenary # 30 (Oct. "03)		Make revised version of full TR.
				SA3 plenary (Nov. . 2003)		Refine the revised version of full TR for submission to SA plenary in Dec '03.
				SA plenary (Dec. 2003)		Submit revised version of TR to SA plenary in Dec. '03, for approval.

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments

11. Work item raporteurs

Raziq Yaqub, Toshiba America Research Inc.

12. Work item leadership

SA3

13. Supporting Companies

Toshiba, Intel, T-Mobile, Nokia, Telcordia, Thomson, Fujitsu, HP, RIM, SmartTrust, BT Group PLC, Alcatel.~~,~~

14. Classification of the WI (if known)

Not Known