

---

**Title:** Work Item Description of a feasibility studying for U(SIM) Re-use Security Requirements For Multiple Network Interfaces  
**Source:** Toshiba, Intel, T-Mobile, Nokia  
**Agenda item:** 7.16 User Equipment Functionality Split  
**Document for:** Discussion/Decision

---

**Work Item Description of a feasibility studying for U(SIM) Re-use Security Requirements For  
Multiple Network Interfaces**

**1. 3GPP Work Area**

	Radio Access
X	Core Network
	Services
X	Terminals

**2. Linked work items**

WLAN security (tbd).

**3. Justification**

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. 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.

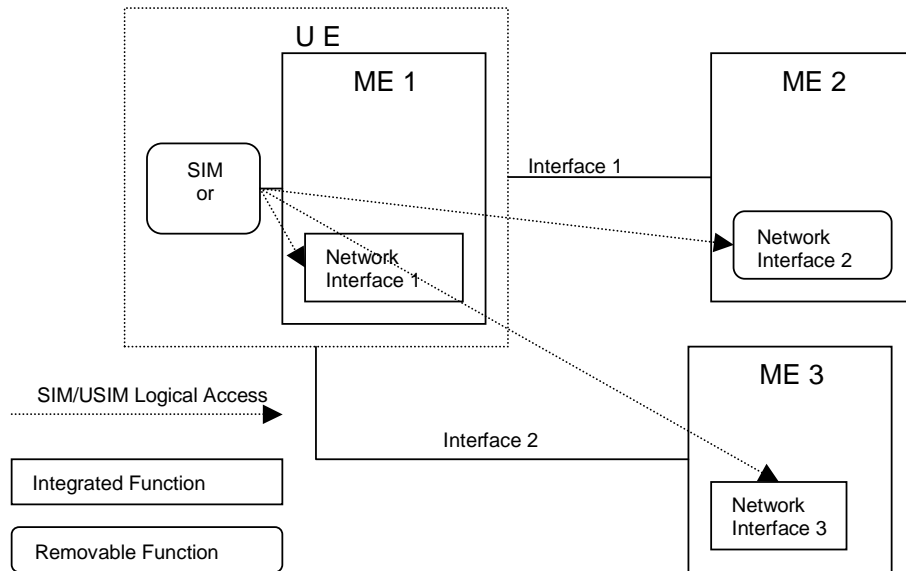


Figure 1: SIM/USIM Re-use Generic Model for Multiple Network Interfaces

**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 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 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.



**11. Work item rapporteurs**

Raziq Yaqub, Toshiba America Research Inc.

**12. Work item leadership**

SA3

**13. Supporting Companies**

Toshiba, Intel, T-Mobile, Nokia, Telcordia, Thomson, Fujitsu, HP, RIM, and SmartTrust.

**14. Classification of the WI (if known)**