3GPP TSG SA WG3 Security – S3#36 **S3-041107**
Shenzhen, 23-26 November 2004

CR-Form-v7

CHANGE REQUEST

⌘ **33.817** **CR** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Update to not rule out the use of the smart card for security enhancements
Source:	⌘	Gemplus
Work item code:	⌘	(U)SIM re-use
Date:	⌘	14/11/04
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*

Reason for change:	⌘	The smart card could be involved in the security mechanisms defined to fulfill the security requirements identified in TR 33.817. So, the TR shall take into account the presence of the smart card.
Summary of change:	⌘	Update to not rule out the use fo the smart card for security enhancements.
Consequences if not approved:	⌘	The smart card could not be involved in the security mechanisms.

Clauses affected:	⌘	

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

BEGIN OF CHANGE

4.4 Issues to be addressed

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 many of the examples illustrated in figure 3, especially in the context of WLAN. This section attempts to capture some of the important issues that need to be addressed for making (U)SIM re-use feasible for the usage scenarios illustrated in figure 3.

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.

- **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 when the (U)SIM is re-used for WLAN authentication over a BT link. 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) that 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.

- **Issue 5**. How many and which kind of UE's should be allowed to have simultaneous access and should the number of UE's be visible to operators?

- **Issue 6**. Which degree of control does the device holding the (U)SIM require on the type of operations that other devices perform with its (U)SIM? What is the role of the UICC?

NOTE: Related to issues 1, 3, and 4: The SIM specification was frozen at Rel-4 and cannot be changed. If any other information (e.g. keys or pseudonyms) is deemed useful to be stored on the UICC, new fields need to be specified. These fields are expected to be both device- and access-specific (e.g. stored WLAN keys are not useful for 3GPP access).

END OF CHANGE

BEGIN OF CHANGE

6 Potential Requirements

According to the proposal, "(U)SIM Security Reuse by Peripheral Devices on Local Interfaces" the (U)SIM card may reside in a 3GPP UE and be accessed by a WLAN-UE through Bluetooth, IR or a USB cable or some other similar wired or wireless interconnect technology. This would facilitate the user to get simultaneous WLAN and 3GPP access with the same (U)SIM. In order to accomplish this, while at the same time addressing the issues and threats mentioned above, following requirements shall be satisfied:

R1. A secured interface between the device holding the (U)SIM and the device with the radio interface is required. This interface must be able to protect against eavesdropping, and undetected modification attacks on security-related signalling data (e.g. authentication challenges and responses). Cryptographic or physical means may be used for this purpose. The UICC may be involved in the security mechanisms to protect the interface.

R2. For cryptographic means, the encryption key length shall be at least 128 bits.

R3. Keys used for local interface transport security should not be shared across local interface links. Each local interface must use unique keys. (For example in Bluetooth, Combination of Link keys shall be used. In case of Bluetooth, the keys may change when a new SIM Access Profile connection is established).

R4. Both endpoints of the local interface shall be mutually authenticated and authorized.

R5. The device without (U)SIM should be capable of discovering the device(s) with (U)SIM in its proximity.

R6. The peripheral device without (U)SIM shall be capable of communicating with the U(SIM) only if the device containing (U)SIM is switched on and a (U)SIM is powered on. Furthermore the device without (U)SIM shall not be allowed to change the status of the device with (U)SIM, or the remote (U)SIM, e.g. to reset it, or to switch its power on or off.

R7. The peripheral device without the (U)SIM shall be capable of detecting the presence and availability of the (U)SIM on the device containing it. It also has the ability to terminate an authenticated network sessions when, the (U)SIM is no longer accessible within a short monitoring time period.

R8. User shall have the capability to shut off sharing of (U)SIM feature. The owner of the device, holding the (U)SIM should authorize its use.

R9. Integrity and privacy of signalling between the WLAN system and the 3GPP core network shall be supported. Leakage of (U)SIM information to the user, or any third party over the wireless interface (Bluetooth/WLAN) is the major security threat. This leakage of information should be guarded against.

R10. Whenever someone tries to remotely access a (U)SIM some sort of alert may be sent, e.g. a message will be displayed informing the user of the access. The user can then decide whether the access is authorized and can allow or disallow it. The security level must be the same or better than present GSM System or as defined by IETF (EAP-SIM, EAP-AKA) and shall apply to Circuit Switched (CS) domain as well as Packet Switched (PS) domain.

R11. It shall be possible to simultaneously access both WLAN and 3GPP radio access technologies, i.e. it should support simultaneous calls on two different air interfaces. For example, the UE might use the WLAN for data services (internet access) together with the 3GPP system for a speech call. The UE and the WLAN and 3GPP systems might elect to use both access technologies simultaneously in order to balance traffic, system capabilities or for radio resource management.

R12. The UICC bearing device should be responsible for serializing access to the (U)SIM Application/Data.

R13. The user should be able to select (U)SIM and TEs as part of their user equipment combination.

R14. A standardized API for access to capabilities provided by an MT (TE) towards a TE (MT) across Operating Systems must be provided.

R15. UICC presence detection shall be supported via the local interface. The local interface may need to address Issue No. 2, e.g. by retransmission of the STATUS command.

R16. Security Reuse shall be consistent with current security arrangements for Release 6 and ensure that user security is not compromised.

R17. Applications/Data information could be retrieved from (U)SIM, provided that (U)SIM is inserted in a 3GPP ME. When the (U)SIM is re-used over local interfaces, further access control on the Applications/Data information should be applied by the 3GPP ME bearing the (U)SIM.

NOTE: This access control, related to Issue No. 6, is ffs.

END OF CHANGE