3GPP TSG SA WG3 Security — S3#37
Sophia Antipolis, France 21 - 25 February 2005

Tdoc ⌘S3-050159

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.234** **CR** **057** ⌘ **rev** **1** ⌘ Current version: **6.3.0** ⌘

*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⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Clarifing the status that can't be changed in the security requirement of WLAN-UE split
Source:	⌘	Nokia, Ericsson
Work item code:	⌘	WLAN
Date:	⌘	10/01/2005
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The meaning of "status" isn't clear in clause 2 in 4.2.4.2. The status was meant to be powering on/off status as agreed in the conference calls in August 2004.
Summary of change:	⌘	State directly the status is powering on/off status.
Consequences if not approved:	⌘	There may be misunderstanding of the meaning of "status".

Clauses affected:	⌘	4.2.4.2

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

Other comments:	⌘	

*** BEGIN OF CHANGE ***

4.2.4.2 Generic security requirements on local interface

The security functionality required on the terminal side for WLAN-3G interworking may be split over several physical devices that communicate over local interfaces. The UICC or the SIM card may reside in a 3GPP UE (acting as a (U)SIM "server") and be accessed by a WLAN-UE through Bluetooth, Infrared or a USB (Universal Serial Bus) cable or some other similar wired or wireless interconnect technology (acting as the (U)SIM "client"). This would facilitate the user to get simultaneous WLAN and 3GPP access with the same (U)SIM. If this is the case, then the following requirements shall be satisfied:

1. Any local interface shall be protected against eavesdropping, attacks on security-relevant information. This protection may be provided by physical or cryptographic means. For cryptographic means, the encryption key length shall be at least 128 bits.

2. The endpoints of a local interface should be authenticated and authorised. The authorisation may be implicit in the security set-up. Keys used for local interface transport security shall not be shared across local interface links. Each local interface shall use unique keys.

3. The involved devices shall be protected against eavesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.

4. The device without (U)SIM shall not be allowed to change the status of the device with (U)SIM, ~~e.g~~i.e. to reset it, or to switch its power on or off.

5. The (U)SIM holding device shall allow the user to shut off sharing of (U)SIM feature.

*** END OF CHANGE ***