3GPP TSG-SA3 #29
San Fransisco, USA, 15-18 July, 2003

Tdoc ⌘S3-030365

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** ⌘ **rev** **-** ⌘ Current version: **0.5.0** ⌘

*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:	⌘	WLAN UE Functional Split
Source:	⌘	Ericsson
Work item code:	⌘	WLAN
Date:	⌘	2003-07-04
Category:	⌘	
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:	⌘	In the case when the WLAN-UE, equipped with a UICC (or SIM card), for accessing the WLAN interworking service, is functionally split over several physical devices, that communicate over local interfaces e.g. Bluetooth, IR or serial cable interface, then is shall be possible to re-use existing UICC and GSM SIM cards; and EAP-AKA and EAP-SIM shall terminate in the TE (e.g. laptop computer). For SIM access via a Bluetooth link, it should be allowed to use the SIM Access Profile developed in BLUETOOTH SIG forum.
Summary of change:	⌘	It shall be: - possible to re-use existing UICC and GSM SIM cards; and - EAP-AKA and EAP-SIM shall terminate in the TE (e.g. laptop computer); in the WLAN UE functional split.
Consequences if not approved:	⌘	SIM access via a Bluetooth link can't be achieved, as SIM Access Profile is the only available protocol for SIM access via Bluetooth.

Clauses affected:	⌘	2, 4.2.4

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

Other comments:	⌘	

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 22.934: " Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking;".

[2] 3GPP TR 23.934: "3GPP system to Wireless Local Area Network (WLAN) Interworking; Functional and architectural definition ".

[3] RFC 2284, March 1998, "PPP Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-06, November 2002, "EAP AKA Authentication".

[5] draft-haverinen-pppext-eap-sim-07, November 2002, "EAP SIM Authentication".

[6] IEEE Std 802.11i/D2.0, March 2002, "Draft Supplement to STANDARD FOR Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".

[7] RFC 2716, October 1999, "PPP EAP TLS Authentication Protocol".

[8] SHAMAN /SHA/DOC/TNO/WP1/D02/v050, 22-June-01, “Intermediate Report: Results of Review, Requirements and Reference Architecture”

[9] ETSI TS 101 761-1 v1.3.1B “Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 1: Basic Data Transport”

[10] ETSI TS 101 761-2 v1.2.1C “Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 2: Radio Link Control (RLC) sublayer”

[11] ETSI TS 101 761-4v1.3.1B “Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 4 Extension for Home Environment”

[12] ETSI TR 101 683 v1.1.1 “Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview”

[13] 3GPP TS 23.234 “3GPP system to Wireless Local Area Network (WLAN) Interworking System Description”.

[14] RFC 2486, January 1999, "The Network Access Identifier"

[15] RFC 2865, June 2000, "Remote Authentication Dial In User Service (RADIUS)"

[16] RFC 1421, February 1993, "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures"

[17] Federal Information Processing Standard (FIPS) draft standard, "Advanced Encryption Standard (AES)", November 2001

[18] 3GPP TS 23.003: "Numbering, addressing and identification"

[19] IEEE P802.1X/D11 June 2001, "Standards for Local Area and Metropolitan Area Networks: Standard for Port Based Network Access Control".

[20] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[21] SIM Access Profile, Interoperability Specification, version 0.95VD - d. Document no. CAR 020 SPEC/0.95cB

---------- Next change ----------

4.2.4 WLAN-UE Functional Split

4.2.4.1 General

In the case when the WLAN-UE, equipped with a UICC (or SIM card), for accessing the WLAN interworking service, is functionally split over several physical devices, that communicate over local interfaces e.g. Bluetooth, IR or serial cable interface, then is shall be:

- Possible to re-use existing UICC and GSM SIM cards; and
- EAP-AKA and EAP-SIM shall terminate in the TE (e.g. laptop computer).

4.2.4.2 Sequirity 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. If this is the case, then the following requirements shall be satisfied:

- Any local interface shall be protected against eavesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.
- The endpoints of a local interface should be authenticated and authorised. The authorisation may be implicit in the security set-up.
- 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.

[Editor's note: New work item approved at SA3#28" U(SIM) Security Reuse by Peripheral Device on local Interfaces" (S3-030307). The Local interface" undetected modification" requirement - cryptographic requirement for short range e.g. Bluetooth is FFS pending the completion of this WI]

4.2.4.3 Communication over local interface via a Bluetooth link

For SIM access via a Bluetooth link, the SIM Access Profile developed in BLUETOOTH SIG forum may be used, see [21].

[Editor note: The version of the SIM Access Profile specification in the reference needs to be updated, if SA3 decides that a new version is required.]