3GPP TSG–SA3 Meeting #25
Munich, Germany, 8-11 October 2002

Tdoc ⌘S3-020521

CR-Form-v7

CHANGE REQUEST

⌘ **33.cde** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **0.1.0** ⌘

*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 [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Editorial changes concerning abbreviations
Source:	⌘	Gemplus
Work item code:	⌘	WLAN Interworking Security
Date:	⌘	02/10/2002
Category:	⌘	**D**
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:	⌘	Errors in the definition of the terms USIM and UICC.
Summary of change:	⌘	New definition of the USIM and UICC terms.
Consequences if not approved:	⌘	Inconsistent use of terminology across documents

Clauses affected:	⌘	Chapters 3.2 and 4.2			
		Y	**N**		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication Authorisation Accounting
AKA	Authentication and key agreement
EAP	Extensible Authentication Protocol
HSS	Home Subscriber Server
MAC	Message Authentication Code
ME	Mobile Equipment
NAI	Network Access Identifier

SIM	Subscriber Identity Module
UE	User Equipment
UICC	~~UMTS IC Card~~ Universal Integrated Circuit Card
USIM	~~UMTS SIM~~ Universal Subscriber Identity Module
WLAN	Wireless Local Area Network

4.2 Security Requirements

[Editor's note: These requirements are copied from TS 23.xxx v0.1.0 for the first version of this TR, and shall be reviewed and updated according to the input from the preceding sections]

- Legacy WLAN terminals should be supported.
- Minimal impact on the user equipment, i.e. client software.
- The need for operators to administer and maintain end user SW should be minimized
- Existing UICC cards should be supported. The solution as such should not require any new changes to the UICC cards.
- Changes in the HSS/HLR/AuC should be minimized.
- The security data, i.e. long-term keys, which are stored on the UICCcard must not be sent from the card itself. Instead the interface to the UICC card should be of type challenge-response, i.e. a challenge is sent to the UICC card and a response is received in return.
- The user should have same security level for WLAN access as for 3GPP access.
- Mutual Authentication should be supported
- The selected Authentication solution should also allow for Authorisation
- Methods for key distribution to the WLAN access NW shall be supported
- Selected WLAN authentication mechanisms for 3GPP interworking shall provide at least the same security as 3GPP System authentication procedure
- Subsequent WLAN re-authentication shall not compromise the requirement for 3GPP System equivalent security
- Selected WLAN Authentication mechanisms for 3GPP interworking shall support agreement of session keying material.
- Selected WLAN key agreement and key distribution mechanism shall be secure against man in the middle attacks. In other words, a man in the middle shall not be able to learn the session key material.
- The WLAN technology specific connection between the WLAN UE and WLAN AN shall be able to utilise the generated keying material for protecting the integrity of an authenticated connection
- It shall be possible to store all long-term security credentials used for subscriber and network authentication in a tamper ~~proof~~ resistant memory such as the UICC card.