3GPP TSG-SA3 Meeting #33
Beijing, China, 10-14 May 2004

Tdoc ⌘S3-040424

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘ **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⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Requirement on keeping WLAN access keys independent from 2G/3G access keys stored in USIM
Source:	⌘	Nokia
Work item code:	⌘	WLAN-3G interworking security
Date:	⌘	14/05/2004
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:	⌘	In SA1's stage-1 specification 22.234, section 5.1.2 USIM and UICC, it is stated: "Access via an I-WLAN shall be possible using earlier releases (than the current release) of the UICC or using a SIM. Access to services via an I-WLAN with a single UICC shall be possible." In SA2's architecture specification 23.234, section 5.1 Access Control, it states the requirement on the smart card as: " - Existing SIM and USIM shall be supported. - Authentication shall rely on (U)SIM based authentication mechanisms. - R6 USIM may include new functionality if necessary e.g. in order to improve privacy." With such requirements, the WLAN specific parameters such as CK and IK (for USIM access) and Kc (for SIM access) cannot be stored in the UICC/SIM (clearly they should not overwrite the corresponding parameters for 2G/3G RAN access).
Summary of change:	⌘	A general description is added to cover all cases specified.
Consequences if not approved:	⌘	WLAN access would result in UE lossing keys for 2G/3G RAN access, and thereby require that the UEs initiate a full authentication at 2G/3G RAN connection establishment, because the key set reads out from the smart card is not correct.

Clauses affected:	⌘	6.1

Y | N

Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

*** START CHANGE***

6 Security mechanisms

6.1 Authentication and key agreement

The WLAN UE and AAA server shall support both EAP AKA and EAP SIM methods. The procedure to select the method is:

1) The WLAN UE shall send an identity (whatever it is: permanent, pseudonym, etc.) to the AAA server. If this identity is an IMSI, it shall contain an indication of the EAP method to be used.

2) If the AAA server recognizes the EAP method but not the user identity (for example an obsolete pseudonym), it shall request a new identity using the EAP method indicated by the WLAN UE.

3) If the AAA server recognizes the user identity (and hence the EAP method), it shall fetch AVs from HSS. If they don't match the EAP method received (e.g. the EAP method received is EAP AKA and triplets are received from HSS), the user's subscription shall prevail (in the previous example EAP SIM shall be used).

4) If the user identity is not recognized, the AAA server shall decide which method to use (there may exist a default method ONLY in this situation). If this default method does not match user's subscription (e.g. EAP AKA for a SIM user), the WLAN UE shall respond a NACK to the AAA server and then the AAA shall try with the other EAP method until a recognised identity is received.

The authentication and key agreement shall be dedicated for WLAN access only, thus the keys provided by the SIM (Kc) or USIM (CK, IK) during authentication shall be stored in the ME’s volatile memory.

*** END OF CHANGE***