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

Tdoc ⌘S3-050017

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**054**	⌘**rev**	**-**	⌘	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:	⌘	WLAN Link Layer Security Descriptions			
Source:	⌘	ZTE Corporation			
Work item code:	⌘	WLAN	***Date:***	⌘	21/01/2005
Category:	⌘	**B**	***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 description of WLAN link layer security requirements is void, and needs completion.
Summary of change:	⌘	Adding three requirements about data protection, signalling protection and key management in WLAN link layer.
Consequences if not approved:	⌘	Specification is not complete.

Clauses affected:	⌘	4.2.5, 4.2.5.1, 4.2.5.2, 4.2.5.3				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN OF CHANGES ***

*** BEGIN OF CHANGES ***

4.2.5 Link layer security requirements

~~Editors note: This section is FFS, LS (S3-030167) sent to SA2 group on 1) the need for requiring 802.11i in TS 23.234. SA2 to explain the impact (if any) a change of technology from 802.11i to WPA would have on the standardisation work. 2) SA2 to study the architectural impacts of implementing protection on Wa interface 3) SA2 to Investigate the importance of specifying specific WLAN technologies to be used for the WLAN access network.~~

Most WLAN technologies provide (optional) link-layer protection of user data. Since the wireless link is likely to be the most vulnerable in the entire system, 3GPP-WLAN interworking should take advantage of the link layer security provided by WLAN technologies. The native link-layer protection can also prevent against certain IP-layer attacks.

Areas in which relevant requirements are defined are:

- ~~Confidentiality and integrity p~~Protection of user data;
- Protection of signalling;
- Key distribution, key freshness validation and key ageing.

These requirements are out of scope of 3GPP. IEEE has defined the security requirements and features for the link layer in WLAN access networks, see IEEE 802.11i [6]. Other WLAN access technologies are not excluded to be used although not described here.

4.2.5.1 ~~Void~~ Protection of user data

User data transmitted over WLAN link layer should be protected against eavesdropping, modification and replay attack; some data protection protocol should be used to achieve this. If IEEE 802.11 is used as WLAN technology, TKIP or CCMP can be used, but WEP is thought not secure enough to be a candidate.

4.2.5.2 ~~Void~~ Protection of signalling

NOTE: signalling protection is FFS. IEEE 802.11i [6] doesn't provide signalling protection of link layer, so there are threats of DoS attacks by replaying some control frames.

4.2.5.3 ~~Void~~ Key distribution, key freshness validation and key ageing

Key materials generated during EAP authentication can be used for link layer data protection directly or by key derivation. EAP authentication methods should ensure the security and freshness of key materials.
Encryption keys for link layer data protection should be aged after some period of time or some volume of traffic encrypted. Before the keys are aged, some mechanism (e.g. UE-AP handshake) should be used to update them.

*** END OF CHANGES ***