3GPP TSG SA WG3 Security — S3#34 *Tdoc ⌘S3-040523*
Acapulco, Mexico 6 - 9 July 2004

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

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

Title:	⌘	Deletion of editor's note
Source:	⌘	Ericsson
Work item code:	⌘	WLAN
Date:	⌘	22/06/2004
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 SA3#33 meeting, BT provided an useful document to track the editor's note in TS 33.234. This CR, together with a discussion paper, proposes the removal of one editor's note. The reasons for the removal are explained in the discussion paper
Summary of change:	⌘	Removal of editor's note *"Threats on the Wa interface are not clear yet, so protection on this interface is for further study."*
Consequences if not approved:	⌘	The editor's note may indicate uncertainties in the security of the Wa interface, which in the discussion paper are proven to not exist.
Clauses affected:	⌘	4.2.2

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

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

*** BEGIN SET OF CHANGES ***

4.2.2 Signalling and user data protection

- The subscriber should have at least the same security level for WLAN access as for his current cellular access subscription.
- 3GPP systems should support authentication methods that support protected success/failure indications.

  Editors note: It is for further study if this is possible.
- The selected WLAN (re-) authentication mechanisms for 3GPP interworking shall provide at least the same level of security as [33.102] for USIM based access.
- The selected WLAN (re-authentication mechanism for 3GPP interworking shall provide at least the same level of security as [43.020] for SIM based access.
- Selected WLAN Authentication mechanisms for 3GPP interworking shall support agreement of session keying material.
- 3GPP systems should provide the required keying material with sufficient length and the acceptable levels of entropy as required by the WLAN subsystem.

  Editors note: LS (S3-030166) sent to IEEE 802.11-task group i on their requirements over key length and entropy of keying material
- Selected WLAN key agreement and key distribution mechanism shall be secure against man in the middle attacks.
- Protection should be provided for WLAN authentication data and keying material on the Wa, Wd and Wx interfaces.
- The WLAN technology specific connection between the WLAN-UE and WLAN AN shall be able to utilise the generated session keying material for protecting the integrity of an authenticated connection.

  ~~Editor's note: Threats on the Wa interface are not clear yet, so protection on this interface is for further study.~~

*** END SET OF CHANGES ***