3GPP TSG SA WG3 Security — S3#34 Tdoc •S3-040603
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 **X**

Title:	•	Clarification on fast re-authentication procedure
Source:	•	Ericsson
Work item code:	•	WLAN
Date:	•	16/06/2004
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:	•	Fast re-authentication procedure is specified in TS 33.234. However, it is not clearly written how the re-use of keys is performed. This CR proposes to specify which keys are re-used and which ones are generated again in the process.
Summary of change:	•	The key derivation process for fast re-authentication is specified.
Consequences if not approved:	•	Misunderstanding of the fast re-authentication process and wrong selection of keys.
Clauses affected:	•	6.1.4

Other specs affected:	•	Y	N		•	
		X		Other core specifications		24.234
			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 ***

6.1.4 Fast re-authentication mechanisms in WLAN Access

When authentication processes have to be performed frequently, it can lead to a high network load especially when the number of connected users is high. Then it is more efficient to perform fast re-authentications. Thus the re-authentication process allows the WLAN-AN to authenticate a certain user in a lighter process than a full authentication, thanks to the re-use of the keys derived on the previous full authentication.

The re-use of keys from previous authentication process shall be performed as follows: the “old” Master Key is fed into a pseudo-random function (as in full authentication) to generate a new Master Session Key (MSK) and a new Extended MSK. In this process, new Transient EAP Keys (TEKs) are generated but shall be discarded. The TEKs, needed to protect the EAP packets, shall be the “old” ones. So the EAP packets shall be protected with the same keys as in the previous full authentication process but the link layer key in the WLAN access network are renewed as the MSK (from which the link layer key is extracted) is generated again.

This process implies that the AAA server, after a full authentication process when a re-authentication identity has been issued, shall store the keys needed in case the next authentication is fast re-authentication: MK, TEKs and Counter (in case there has been previous fast-authentications). When the WLAN UE has completed a full authentication where it has received the re-authentication identity, it shall store the same data in order to be prepared for fast re-authentication.

*** END SET OF CHANGES ***