3GPP TSG SA WG3 Security — S3#23

14 - 17 May 2002, Victoria, Canada

S3-020284

CR-Form-v5

CHANGE REQUEST

| ⌘ | **33.203** CR | ⌘rev | **-** | ⌘ | Current version: | **5.1.0** | ⌘ |

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Update of User Authentication Failure
Source:	⌘	Hutchison 3G UK
Work item code: ⌘		*Date:* ⌘ 09/05/02

Category:	⌘ **F**	*Release:* ⌘ Rel-5

Use <u>one</u> 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 <u>one</u> 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)

Reason for change:	⌘	The text is updated to account for using Digest AKA, as RES is no longer directly checked. It also describes what to do if the integrity protection passes and the response fails.
Summary of change:	⌘	The text is changed to make it the authentication response that is checked as opposed to the RES. It also describes what happens in the unlikely circumstances that the integrity check passes but the response fails.
Consequences if not approved:	⌘	The text will not reflect the use of Digest AKA to carry the authentication response. No behaviour will be described in the unlikely event that the integrity check passes but the authentication response fails. Both issues could lead to incorrect implementations.

Clauses affected:	⌘	6.1.2, 6.1.2.1

Other specs affected:	⌘ ☐	Other core specifications	⌘
	☐	Test specifications	
	☐	O&M Specifications	

Other comments:	⌘	

6.1.2 Authentication failures

6.1.2.1 User authentication failure

In this case the authentication of the user should fail at the S-CSCF due an incorrect responseRES (received in SM9). However, in theis case when the responseRES is incorrect, it is very likely that the IK used to protect SM7 will be incorrect as well, which will cause the and integrity check at the P-CSCF towill fail before the response canRES can be verified at S-CSCF. In this case the

P-CSCF in this case shall discard SM7 and the registration and authentication procedures shall be then aborted.

If the integrity check passes but the response is incorrect, the message flows are identical up to and including SM9 as a successful authentication. Once the S-CSCF detects the user authentication failure it should proceed in the same way as having received SM9 in a network authentication failure (see clause 6.1.2.2).