3GPP TSG SA #6 **Tdoc TSG SA SP-99590**
Nice, FRANCE
15th - 17th December 1999

Source: TSG SA WG3

Subject: R99 CR to 21.133
Agenda item: 5.3.3

This document contains a CR to 21.133 version 3.0.0 agreed by SA WG3 to be presented to SA#6 for approval.

CR	REV	CAT	SUBJECT	WG_DOC	3G_PHASE
001		C	Data integrity of user traffic	S3-99450	99

TSG SA WG3 #8, Sophia Antipolis, 16—19 November, 1999 **S3-99450**

DRAFT 3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

TS 21.133 **CR** **001** Current Version: V3.0.0

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG SA#6 for approval ☒ *(only one box should*
list TSG meeting no. here ↑ for information □ *be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: USIM □ ME ☒ UTRAN ☒ Core Network □
(at least one should be marked with an X)

Source:	3GPP TSG SA WG3	**Date:**	18-11-99
Subject:	Data integrity of user traffic		
3G Work item:	Security		

Category:
(only one category shall be marked with an X)

F	Correction	□
A	Corresponds to a correction in a 2G specification	□
B	Addition of feature	□
C	Functional modification of feature	☒
D	Editorial modification	□

Reason for change: Notes are added to clarify that the requirement for data integrity and data origin authentication of user traffic is compatible with the absence of a separate security feature and mechanism for those purposes, because the stream cipher is considered to provide sufficient integrity protection.

Clauses affected: Clause 8

Other specs affected:

Other 3G core specifications	□	→ List of CRs:
Other 2G core specifications	□	→ List of CRs:
MS test specifications	□	→ List of CRs:
BSS test specifications	□	→ List of CRs:
O&M specifications	□	→ List of CRs:

Other comments:

help.doc

<---------- double-click here for help and instructions on how to create a CR.

8.1.1 Requirements on security of 3GPP services

8.1.1.1 Requirements on secure service access

R1a A valid USIM shall be required to access any 3G service except for emergency calls where the network should be allowed to decide whether or not emergency calls should be permitted without a USIM. (T7d, T9a,d)

R1b It shall be possible to prevent intruders from obtaining unauthorised access to 3G services by masquerading as authorised users. (T4a, T9a,c)

R1c It shall be possible for users to be able to verify that serving networks are authorised to offer 3G services on behalf of the user's home environment at the start of, and during, service delivery. (T1c,e, T3c, T4a, T9b,c)

8.1.1.2 Requirements on secure service provision

R2a It shall be possible for service providers to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorised access to 3G services by masquerade or misuse of priorities. (T4a, T8a, T9a,d)

R2b It shall be possible to detect and prevent the fraudulent use of services. Alarms will typically need to be raised to alert providers to security-related events. Audit logs of security related events will also need to be produced. (T8a,b,c, T9d,e, T10a,b)

R2c It shall be possible to prevent the use of a particular USIM to access 3G services. (T9a,d, T10a)

R2d It shall be possible for a home environment to cause an immediate termination of all services provided to certain users, also those offered by serving networks. (T9a,d, T10a,b)

R2e It shall be possible for the serving network to be able to authenticate the origin of user traffic, signalling data and control data on radio interfaces. (T8a,b,c, T9c)

Note: It is assumed that user traffic contains sufficient redundancy such that a stream cipher provides a basic level of data origin authentication on the radio interfaces and that, if that is not sufficient and additional measures are required, the application should be aware and measures should be implemented at the application layer.

R2f It shall be possible to prevent intruders from restricting the availability of services by logical means. (T3b,c, T7e)

R2g There shall be a secure infrastructure between network operators, designed such that the need for HE trust in the SN for security functionality is minimised.

8.1.2 Requirements on system integrity

R3a It shall be possible to protect against unauthorised modification of user traffic. (T2a, T6a,c, T7b,c)

Note: It is assumed that user traffic contains sufficient redundancy such that a stream cipher provides a basic level of data integrity protection on the radio interfaces and that, if that is not sufficient and additional measures are required, the application should be aware and measures should be implemented at the application layer.

R3b It shall be possible to protect against unauthorised modification of certain signalling data and control data, particularly on radio interfaces. (T2b, T3b,c, T6b,c, T7a,b,c)

R3c It shall be possible to protect against unauthorised modification of user-related data downloaded to or stored in the terminal or in the USIM. (T6d,e, T6c, T10f,i)

R3d It shall be possible to protect against unauthorised modification of user-related data which is stored or processed by a provider. (T6c,f)

R3e It shall be possible to ensure that the origin and integrity of applications and/or data downloaded to the terminal and/or the UICC can be checked. It may also be necessary to ensure the confidentiality of downloaded applications and/or data. (T6c,d,e,f, T10e,f,i)

R3f It shall be possible to ensure the origin, integrity and freshness of authentication data, particularly of the cipher key on the radio interface. (T1a,b, T2b, T5c, T6c)

R3g It shall be possible to secure infrastructure between operators. (T5a,b,c, T6a,b,c, T7a,b,c, T9b,c)