3GPP TSG SA WG3 Security — S3#16 **S3-000657**

28-30 November, 2000

Sophia Antipolis, France

3GPP TSG-CN4 **Tdoc N4-001062**
#05 Meeting, Paris, FRANCE
13th November – 17th November 2000

Title:	LS on Clarifications to the Security Mode usage, and error cases
Source:	TSG_CN WG4
To:	TSG_SA WG2
Cc:	TSG_SA WG3

Contact Person:

Name:	**Ahti Muhonen**
E-mail Address:	**Ahti.Muhonen@nokia.com**
Tel. Number:	+358 (40) 5318469

CN4 kindly asks TSG SA WG2 to consider the attached CR against 23.060 with the subject: Annex to LS to SA2 on clarifications to the security function. The contribution defines selection rules for an old SGSN on the type of MM Context it shall send to a new SGSN in the SGSN Context Response message.

Attachments:

N4-001063

The next CN4 meeting

The next CN4 meeting will be held 15th – 19th January 2001 in Beijing.

3GPP-CN4 Meeting # 5
Paris, France 13-17 November 2000

Document ***N4-001063***

e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

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

23.060 **CR** Current Version: 3.5.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: SA#10 for approval ☒ Strategic □ *(for SMG use only)*
list expected approval meeting # here ↑ for information □ non-strategic □

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

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

Source: CN4 **Date:** 14 November 2000

Subject: Annex to LS to SA2 on clarifications to the security function

Work item: Security

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

F	Correction	☒	**Release:**	Phase 2	□
A	Corresponds to a correction in an earlier release	□		Release 96	□
B	Addition of feature	□		Release 97	□
C	Functional modification of feature	□		Release 98	□
D	Editorial modification	□		Release 99	☒
				Release 00	□

Reason for change:

"Note: the comments within double quotes are only for discussion in CN4 #5. Please remove these from the version that might be sent to S2.

I have faced a dilemma of either proposing to scatter changes to RAU and intersystem change sub clauses, as one option, or of proposing to limit the changes to section 6.8.1, as another one. For clarity reasons, I have chosen the latter option. However, in case N4 find my choice inappropriate, I'll readily provide the other version of the contribution. Besides, it was not clear for me how to handle the CR number issue. Hence, I left the field blank"

33.102v3.6.0 allows an old SGSN to send one of the security type MM contexts to the new SGSN in the SGSN Context Response message.

It is proposed to clarify what security type MM context a SGSN should consider as a primary option by explicit definition of the rules in line with 33.102v3.6.0.

Clauses affected: 6.8.1

Other specs affected:

Other 3G core specifications	□	→ List of CRs:	
Other GSM 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.

6.8.1 Authentication

The Authentication function includes two types of authentication: "UMTS authentication" and "GSM authentication".

"UMTS authentication" implies mutual authentication, i.e., authentication of the MS by the network and authentication of the network by the MS. It also implies establishment of a new UMTS ciphering key (CK) and integrity key (IK) agreement between the SGSN and the MS.

"GSM authentication" implies authentication of the MS by the network and establishment of a new GSM ciphering key (Kc) agreement between the SGSN and the MS.

The following rules shall apply for the old SGSN once sending the SGSN Context Response message to the new SGSN.

Security Mode with value 1, or a Security type 1 shall always be used for a GSM subscriber, and never for an UMTS subscriber.

Note: New SGSN determines the type of subscription, by the type of authentication vectors received via SGSN Context Response message. An array of Triplets in MM Context indicate a GSM subscriber, while an array of Quintuplets indicate the UMTS subscriber.

Security types 0, 2 and 3 shall not be used for a GSM subscriber.

For an UMTS subscriber, the primary choice for the old SGSN shall be MM Context with Security Type 0. If the old 3G-SGSN does not have valid value for the Used Cipher, then it shall send MM Context with Security Type 2.

Note: 3G-SGSN marks the Used Cipher as having valid value, if it receives the MM Context with Security Type 0. However, if 3G-SGSN performs AKA, it marks the Used Cipher value as invalid.

Security Type 3 may be used by 2G-SGSN. However, if 3G-SGSNreceives MM Context with Security type 3, AKA shall be performed in order to avoid the second time key conversion.

Note: Sending the SGSN Context Response message with the Security Type 3 MM Context should be avoided. That will decrease the overall number of both local and remote (HLR query) AKA. Besides, there would not be any need in checking the presence of TLLI information element in the SGSN Context Request message.