Technical Specification Group Services and System Aspects *TSGS#5(99)496*

(=S3-99352, rev. of S3-99345)

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 33.102 **CR** **21** Current Version: V3.1.0

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

For submission to TSG SA#5 for approval **X** *(only one box should be marked with an X)*

list TSG meeting no. here ↑ for information

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 **X** ME UTRAN Core Network **X**

(at least one should be marked with an X)

Source: S3 **Date:** 01-10-99

Subject: A generalised scheme for sequence number management

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	X
D	Editorial modification	

Reason for change: Sequence number management as described in the current version of TS 33.102 has drawbacks which the generalised scheme avoids.

Clauses affected: Annex C

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.

Annex C: Management of sequence numbers

This annex is devoted to the management of sequence numbers for the authentication and key agreement protocol.

C.6 A generalised scheme for sequence number management

This section describes the use of generalised sequence numbers which have an individual and a global component.

(1) The sequence number consists of two concatenated parts $SQN = SQN1 \| SQN2$. $SQN1$ represents the most significant bits of SQN, and $SQN2$ represents the least significant bits of SQN.

(2) There are counters SQN_{MS} and SQN_{HE} in the MS and the HE respectively. Both parts of SQN are stored by these counters. SQN_{HE} is an individual counter, i.e. there is one per user.

(3) There is a global counter, e.g. a universal clock with an appropriate time granularity (e.g. seconds elapsed since the start of the system). For short we call the value of this global counter at any one time GLC. If GLC is taken from a universal clock it is computed mod 2^n where n is the length of GLC and of SQN2 in bits.

(4) When the HE needs a new sequence number SQN to create a new authentication vector, HE retrieves the (user-specific) value of $SQN_{HE} = SQN1_{HE} \| SQN2_{HE}$ from the database. If $SQN2_{HE} < GLC$ then HE sets $SQN = SQN1_{HE} \| GLC$. If $SQN2_{HE} \geq GLC$ then HE sets $SQN = (SQN1_{HE} + 1) \| GLC$.
Then SQN_{HE} is reset to SQN.

(5) The sequence number SQN is accepted by the USIM if and only if $SQN > SQN_{MS}$ holds.

(6) If the mechanism described in Annex C.4 (lists of sequence numbers in the USIM) is used and if SQN_{LO} denotes the lowest sequence number in the list then (5) becomes:

The sequence number SQN is now accepted by the USIM if and only if $SQN > SQN_{LO}$ holds and SQN is not in the list.

(7) If the mechanism described in Annex C.5 (protection against counter wrap-around) is employed then (5) becomes:

The sequence number SQN is now accepted by the USIM if and only if $SQN > SQN_{MS}$ and $SQN - SQN_{MS} < \Delta$ hold.

(8) If both the mechanisms described in Annexes C.4 and C.5 are employed and if SQN_{HI} denotes the highest sequence number in the list then (5) becomes:

The sequence number SQN is now accepted by the USIM if and only if $SQN > SQN_{LO}$ and $SQN - SQN_{HI} < \Delta$ hold and SQN is not in the list.

When parameters are appropriately chosen then this use of sequence numbers is compatible with the re-synchronisation procedure described in section 6.3.5 and the protection against wrap around of counters described in Annex C.5, and it is not required to conceal this type of sequence numbers.