Technical Specification Group Services and System Aspects
Meeting #14, Kyoto, Japan, 17-20 December 2001

TSGS#14(01)0608

Source: **SA WG3**

Title: **2 CRs to 33.102: Annex F.2 (changing list parameters) modification (Rel-99 and Rel-4)**

Document for: **Approval**

Agenda Item: **7.3.3**

Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New	Doc-2nd-Level
21.133	156		Rel-99	F	Annex F.2 (changing list parameters) modification	3.9.0	3.10.0	S3-010455
21.133	157		Rel-4	A	Annex F.2 (changing list parameters) modification	4.2.0	4.3.0	S3-010456

3GPP TSG SA WG3 Security — S3#20 **S3-010455**

16-19 October 2001, Sidney, Australia

CR-Form-v4

CHANGE REQUEST

⌘ **33.102 CR 156** ⌘ ev **-** ⌘ Current version: **3.9.0** ⌘

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 ☒

Title:	⌘	Annex F.2 (changing list parameters) modification		
Source:	⌘	SA WG3		
Work item code:	⌘	SEC1	***Date:*** ⌘	19 September 2001
Category:	⌘	**F**	***Release:*** ⌘	R99
		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)*

Reason for change:	⌘	A mechanism in Annex C was changed at S3#15 (Sept 00). Annex F.2 is related to that mechanism, but it was overlooked to bring it in line with the new Annex C.
Summary of change:	⌘	Bring Annex F.2 in line with Annex C.
Consequences if not approved:	⌘	Annex F.2 is not consistent with Annex C.

Clauses affected:	⌘	Annex F	
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments:	⌘		

Annex F (informative): Example uses of AMF

F.1 Support multiple authentication algorithms and keys

A mechanism to support the use of multiple authentication and key agreement algorithms is useful for disaster recovery purposes. AMF may be used to indicate the algorithm and key used to generate a particular authentication vector.

The USIM keeps track of the authentication algorithm and key identifier and updates it according to the value received in an accepted network authentication token.

F.2 Changing sequence number verification ~~list~~ parameters

This mechanism~~s~~ is used in conjunction with the ~~window and list~~ mechanism for the verification of sequence number freshness in the USIM ~~s~~ described in C.2.2.

The USIM shall also be able to put a limit *L* on the difference between SEQ_{MS} (the highest SEQ accepted so far) and a received sequence number *SEQ*. ~~Parameters which may be used to manage a lsit are the number of entries in a list (the list size) and an upper list on the admissible SEQ_{MS} – SEQ between the highest batch number SEQ_{MS} in the list and an accepted batch number SEQ.~~ A mechanism to change this~~these~~ parameter *L*~~s~~ dynamically is useful since the optimum for these parameters may change over time. AMF is used to indicate a new value of *L* to be used by the USIM.~~the maximum admissible list size or maximum admissible difference SEQ_{MS} – SEQ to be used by the user when verifying the authentication token and deciding whether it is still accepted.~~

~~The USIM keeps track of the maximum admissible list size and maximum admissible difference SEQ_{MS} – SEQ and updates them according to the received value providing that $SEQ > SEQ_{MS}$.~~

F.3 Setting threshold values to restrict the lifetime of cipher and integrity keys

According to section 6.4.3, the USIM contains a mechanism to limit the amount of data that is protected by an access link key set. The AMF field may be used by the operator to set or adjust this limit in the USIM. For instance, there could be two threshold values and the AMF field instructs the USIM to switch between them.

The USIM keeps track of the limit to the key set life time and updates it according to the value received in an accepted network authentication token.

3GPP TSG SA WG3 Security — S3#20 **S3-010456**

16-19 October 2001, Sidney, Australia

CR-Form-v4

CHANGE REQUEST

⌘ **33.102 CR 157** ⌘ ev **-** ⌘ Current version: **4.2.0** ⌘

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 ☒

Title:	⌘	Annex F.2 (changing list parameters) modification	
Source:	⌘	SA WG3	
Work item code:	⌘	SEC1	***Date:*** ⌘ 19 September 2001
Category:	⌘	**A** *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.	***Release:*** ⌘ REL-4 *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)*

Reason for change:	⌘	A mechanism in Annex C was changed at S3#15 (Sept 00). Annex F.2 is related to that mechanism, but it was overlooked to bring it in line with the new Annex C.
Summary of change:	⌘	Bring Annex F.2 in line with Annex C.
Consequences if not approved:	⌘	Annex F.2 is not consistent with Annex C.

Clauses affected:	⌘	Annex F	
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments:	⌘		

Annex F (informative): Example uses of AMF

F.1 Support multiple authentication algorithms and keys

A mechanism to support the use of multiple authentication and key agreement algorithms is useful for disaster recovery purposes. AMF may be used to indicate the algorithm and key used to generate a particular authentication vector.

The USIM keeps track of the authentication algorithm and key identifier and updates it according to the value received in an accepted network authentication token.

F.2 Changing sequence number verification ~~list~~ parameters

This mechanism~~s~~ is used in conjunction with the ~~window and list~~ mechanism for the verification of sequence number freshness in the USIM ~~s~~ described in C.2.2.

The USIM shall also be able to put a limit L on the difference between SEQ_{MS} (the highest SEQ accepted so far) and a received sequence number SEQ. ~~Parameters which may be used to manage a lsit are the number of entries in a list (the list size) and an upper list on the admissible $SEQ_{MS} - SEQ$ between the highest batch number SEQ_{MS} in the list and an accepted batch number SEQ.~~ A mechanism to change this~~these~~ parameter L~~s~~ dynamically is useful since the optimum for these parameters may change over time. AMF is used to indicate a new value of L to be used by the USIM.~~the maximum admissible list size or maximum admissible difference $SEQ_{MS} - SEQ$ to be used by the user when verifying the authentication token and deciding whether it is still accepted.~~

~~The USIM keeps track of the maximum admissible list size and maximum admissible difference $SEQ_{MS} - SEQ$ and updates them according to the received value providing that $SEQ > SEQ_{MS}$.~~

F.3 Setting threshold values to restrict the lifetime of cipher and integrity keys

According to section 6.4.3, the USIM contains a mechanism to limit the amount of data that is protected by an access link key set. The AMF field may be used by the operator to set or adjust this limit in the USIM. For instance, there could be two threshold values and the AMF field instructs the USIM to switch between them.

The USIM keeps track of the limit to the key set life time and updates it according to the value received in an accepted network authentication token.