

## CHANGE REQUEST

⌘ **33.102** CR \_\_\_\_\_ ⌘ 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

<b>Title:</b>	⌘	Annex F.2 (changing list parameters) modification	
<b>Source:</b>	⌘	Siemens	
<b>Work item code:</b>	⌘	Security	<b>Date:</b> ⌘ 19 September 2001
<b>Category:</b>	⌘	<b>F</b>	<b>Release:</b> ⌘ R99
		Use <u>one</u> of the following categories:	Use <u>one</u> of the following releases:
		<b>F</b> (correction)	2 (GSM Phase 2)
		<b>A</b> (corresponds to a correction in an earlier release)	R96 (Release 1996)
		<b>B</b> (addition of feature),	R97 (Release 1997)
		<b>C</b> (functional modification of feature)	R98 (Release 1998)
		<b>D</b> (editorial modification)	R99 (Release 1999)
		Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .	REL-4 (Release 4)
			REL-5 (Release 5)

<b>Reason for change:</b>	⌘	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.
<b>Summary of change:</b>	⌘	Bring Annex F.2 in line with Annex C.
<b>Consequences if not approved:</b>	⌘	Annex F.2 is not consistent with Annex C.

<b>Clauses affected:</b>	⌘	Annex F
<b>Other specs affected:</b>	⌘	<input type="checkbox"/> Other core specifications      ⌘ _____ <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications
<b>Other comments:</b>	⌘	_____

---

## 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 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 list are the number of entries in a list (the list size) and an upper limit 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 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.