3GPP TSG-T (Terminals) Meeting #11
Palm Springs, USA, 14 - 16 March, 2001

Tdoc TP-010037

Source: T3

Title: Change Request to TS 03.48 "Security Mechanisms for the SIM application toolkit"

Document for: Approval

This document contains change requests to GSM 03.48 v8.3.0 agreed by T3.

T3 Doc	Spec	CR	Rv	Rel	Subject
T3-010107	03.48	A015		R99	Clarification of the Anti Replay Counter management

3GPP T3 (USIM) Meeting #17
Berlin, Germany, 15 - 17 January, 2001

Tdoc T3-010107
(revised version of T3-010084)

CR-Form-v3

CHANGE REQUEST

⌘	**03.48**	**CR**	**A015**	⌘	rev	**-**	⌘	Current version:	**8.4.0** ⌘

*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:	⌘	Clarification of the Anti Replay Counter management		
Source:	⌘	T3		
Work item code:	⌘		***Date:*** ⌘	17 January 2001
Category:	⌘	**F**	***Release:*** ⌘	R99
		Use one of the following categories: ***F*** *(essential 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:	⌘	The specification allows different interpretation of the Anti Replay Counter management where some may lead to a denial of service by blocking the counter. Additionally, as the counter is part of the certified data, the value can only be considered as valid after its integrity has been checked, so after the MAC has been checked.
Summary of change:	⌘	Clarify when the Anti Replay Counter has to be incremented.
Consequences if not approved:	⌘	

Clauses affected:	⌘	§5.1.4		
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘	
Other comments:	⌘			

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.1.4 Counter Management

The following rules shall apply to counter management, with the goal of preventing replay and synchronisation attacks:

- The SE sets the counter value. It shall only be incremented.

~~- When the counter value reaches its maximum value the counter is blocked .~~

- ~~In order to prevent replay attacks t~~The RE shall increment the counter to its next value upon receipt of a Command Packet after the corresponding security checks (i.e. RC/CC/DS and CNTR verification) have been passed successfully. ~~irrespective of whether or not the Command Packet could be successfully unpacked.~~

- When the counter value reaches its maximum value the counter is blocked.

If there is more than one SE, care has to be taken to ensure that the counter values remain synchronised between the SE's to what the RE is expecting, irrespective of the transport mechanism employed.

The level of security is indicated via the proprietary interface between the Sending/Receiving Application and Sending/Receiving Entity. Application designers should be aware that if the Sending Application requests "No RC/CC/DS" or "Redundancy Check" and "No Counter Available" from the SE, no security is applied to the Application Message and therefore there is an increased threat of malicious attack.