3GPP TSG SA WG3 Security — S3#37
Sophia Antipolis, France 21 - 25 February 2005

Tdoc ⌘S3-050034

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **034** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Storing SP payload after MSK message is verified
Source:	⌘	ZTE Corporation
Work item code:	⌘	MBMS
Date:	⌘	10/01/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	It is insecure to store SP payload in ME before MSK message is verified. SP payload should be stored in ME after MSK message is verified.
Summary of change:	⌘	Changing the corresponding description in clause 6.4.6.1.
Consequences if not approved:	⌘	The procedure of MSK message reception in ME is insecure.

Clauses affected:	⌘	6.4.6.1

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘

*** BEGIN OF CHANGE ***

6.4.6 Processing of received messages in the ME

6.4.6.1 MSK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of RFC 3830 [9]).

1. The Extension Payload (EXT) is examined, and if it indicates an MSK delivery protected with MUK, the MUK ID is received by combining IDi and IDr.
2. The Timestamp Payload is checked, and the message is discarded if the counter in the Timestamp Payload is smaller or equal to the stored replay counter associated with the given MUK (the stored replay counter value is retrieved from MGV-S). To avoid issues with wrap around of the ID fields "smaller than" should be in the sense of RFC 1982 [10].
3. ~~The Security Policy payload is stored if it was present.~~The Security Policy payload is stored in cache of ME if it was present. The SP payload will not be used to update the security policy stored in ME at this moment.
4. The message is transported to MGV-F for further processing, cf clause 6.5.2.
5. The MGV-F replies success or failure. If MGV-F replies success, Security Policy payload stored in cache will be used to update the security policy stored in ME. If MGV-F replies failure, Security Policy payload stored in cache will be deleted.

*** END OF CHANGE ***