

CHANGE REQUEST

33.246 CR 053 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:	Removing IDi from MTK message		
Source:	Ericsson		
Work item code:	MBMS	Date:	14/2/2005
Category:	C	Release:	Rel-6
Use <u>one</u> 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 <u>one</u> 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:	The usage of ID payloads in MIKEY messages was agreed in S3-041097 and implemented in S3-041127. However, S3-041127 did not remove the IDi payload from MIKEY MTK message although this was agreed in S3-041097. This CR aligns the TS 33.246 to the agreed decisions made.
Summary of change:	The IDi payload is removed from MTK message.
Consequences if not approved:	The IDi payload is carried unnecessarily in MTK message.

Clauses affected:	6.4.5.3										
Other specs Affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"> </td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"> </td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"> </td> <td style="padding: 2px;">N</td> </tr> </table>	Y	N		N		N		N	Other core specifications	
	Y	N									
		N									
	N										
	N										
	N	Test specifications									
	N	O&M Specifications									
Other comments:											

******* NEXT CHANGE *********6.4.5.3 MTK message structure**

The structure of the MIKEY message carrying a MTK key is depicted in Figure 6.7. The actual key that is delivered is kept in the KEMAC payload. [The EXT payload has format as described in clause 6.4.4.](#) If MTK is to be used for streaming protection, then a 112 bit salt shall be added to the KEMAC payload in addition to the MTK. ~~The network identity payloads (IDi) shall be used in MTK transport messages.~~

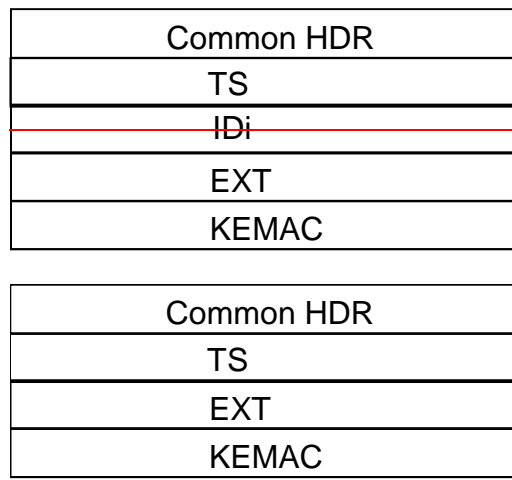


Figure 6.7: The logical structure of the MIKEY message used to deliver MTK