CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **33.246 CR 012** | ⌘**rev** | **1** | ⌘ | Current version: | **6.0.0** | ⌘ |

*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⌘ **X**   ME **X** Radio Access Network ☐ Core Network **X**

Title: ⌘	Clarify the use of mandatory MIKEY features for MBMS	
Source: ⌘	Siemens	
Work item code: ⌘	MBMS	***Date:*** ⌘ 16/11/2004
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: ⌘	MIKEY (IETF: "MIKEY: Multimedia Internet KEYing", http://www.ietf.org/internet-drafts/draft-ietf-msec-mikey-08.txt, Work In Progress.) specifies 1) in clause 3.2 that the public key encryption method is mandatory to implement. 2) in clause 6.6 that Timestamps payload types NTP-UTC and NTP are mandatory to implement The above functionality is not needed for MBMS key management, so there can be doubt if the MBMS implementation is standard compliant if it has not realized the above functions when reading the MIKEY RFC. Explicitly mentioning the not needed mandatory functions in the MBMS TS - require less effort then listing all required functions and payloads - allow faster time to market as there will be no doubt about the (not) required MIKEY features
Summary of change: ⌘	Specify in a new Annex the not required mandatory MIKEY functionality
Consequences if not approved: ⌘	It will remain unclear if the MBMS UE and BM-SC shall implement certain MIKEY features.

Clauses affected: ⌘	New Annex	

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

Other comments: ⌘	

Annex E (Informative): MIKEY features not used in MBMS [9].

- An MBMS capable ME/UICC and BM-SC do not need to implement the public key encryption method of MIKEY (clause 3.2 of [9]) and related payloads, although mentioned in [9] as mandatory for implementation.

- An MBMS capable ME/UICC and BM-SC do not need to implement the Time Stamp payload types NTP-UTC and NTP of MIKEY (clause 6.6 of [9]) although mentioned in [9] as mandatory for implementation.