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

Tdoc ⌘ S3-050137

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**057**	⌘ **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:	⌘	Introduction of missing abbreviations, symbols and defintions
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	24/02/2005
Category:	⌘	**D**
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:	⌘	Some abbreviations, terminology, and symbols used in TS 33.246 are not defined.
Summary of change:	⌘	Missing abbreviations, symbols and defintions are introduced
Consequences if not approved:	⌘	Ambiguity in the specification

Clauses affected:	⌘	3.1, 3.2, 3.x(new)				
		Y	**N**			
Other specs Affected:	⌘		**N**	Other core specifications	⌘	
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply.

For the definitions of MBMS User Service refer to TS 22.246 [5].

HDR = the general MIKEY HeaDeR

KEMAC = A payload included in the MIKEY message, which contains a set of encrypted sub-payloads and a MAC

MBMS download session: See TS 26.346 [13].

MBMS streaming session: See TS 26.346 [13].

MRK = MBMS Request Key: This key is to authenticate the UE to the BM-SC when performing key requests etc.

MSK = MBMS Service Key: The MBMS Service key that is securely transferred (using the key MUK) from the BM-SC towards the UE. The MSK is not used directly to protect the MBMS User Service data (see MTK).

MTK = MBMS Traffic Key: A key that is obtained by the UICC or ME by calling a decryption function MGV-F with the MSK. The key MTK is used to decrypt the received MBMS data on the ME.

MUK = MBMS User Key: The MBMS user individual key that is used by the BM-SC to protect the point to point transfer of MSK's to the UE.

NOTE: The keys MSK and MUK may be stored within the UICC or the ME depending on the UICC capabilities.

Salt key = a random or pseudo-random string used to protect against some off-line pre-computation attacks on the underlying security protocol

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

B-TID	Bootstrapping Transaction Identifier
BM-SC	Broadcast-Multicast Service Centre
BSF	Bootstrapping Server Function
DCF	DRM Content Format
DRM	Digital Rights Management
EXT	Extension payload
FDT	FLUTE File Delivery Table
FLUTE	File delivery over Unidirectional Transport
GBA	Generic Bootstrapping Architecture
GBA_ME	ME-based GBA
GBA_U	GBA with UICC-based enhancements
IDi	Identity of the initiator
IDr	Identity of the responder
Ks_ext_NAF	Derived key in GBA_U
Ks_int_NAF	Derived key in GBA_U, which remains on UICC
Ks_NAF	Derived key in GBA_ME
MAC	Message authentication code
MBMS	Multimedia Broadcast/Multicast Service
MGV-F	MBMS key Generation and Validation Function
MGV-S	MBMS key Generation and Validation Storage
MIKEY	Multimedia Internet Keying
MKI	Master Key identifier
MRK	MBMS Request Key
MSK	MBMS Service Key
MSK_C	Confidentiality key derived from key MSK
MSK_I	Integrity key derived from key MSK
MTK	MBMS Traffic Key
MUK	MBMS User Key
MUK_C	Confidentiality key derived from key MUK
MUK_I	Integrity key derived from key MUK
NAF	Network Application Function
OMA	Open Mobile Alliance
ROC	Roll-over counter

SP	Security Policy
SRTP	Secure RTP

3.x Symbols

For the purposes of the present document, the following symbols apply:

|| Concatenation