3GPP TSG-SA3 Meeting #36
Shenzen, China, 23-26 November 2004

Tdoc ⌘S3-041116

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **016** ⌘ **rev** **3** ⌘ 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:	⌘	Scope of MBMS security
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	15/11/2004
Category:	⌘	**C**
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:

2	*(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)*

Reason for change:	⌘	The Scope of MBMS security is not inline with SA4.
Summary of change:	⌘	The scope of MBMS security is aligned with SA4 to be based on MBMS Streaming/Download Sessions, not on Transport Services.
Consequences if not approved:	⌘	The scope of MBMS security remains incorrect.

Clauses affected:	⌘	2, 3.1, (new) 4.x, 4.2

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

Other comments: ⌘

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.146: "Multimedia Broadcast/Multicast Service; Stage 1".

[3] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 22.246: "MBMS User Services".

[6] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[7] 3GPP TS 31.102: "Characteristics of the USIM application".

[8] IETF RFC 2617 "HTTP Digest Authentication".

[9] IETF RFC 3830 "MIKEY: Multimedia Internet KEYing"

[10] IETF RFC 1982 "Serial Number Arithmetic".

[11] IETF RFC 3711 "Secure Real-time Transport Protocol".

[12] 3GPP TS 43.020: "Security related network functions".

[13] TS 26.346: “Multimedia Broadcast/Multicast Service, Protocols and codecs”

******* NEXT CHANGE *******

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply.

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

MBMS download session: See TS 26.346: “Multimedia Broadcast/Multicast Service, Protocols and codecs” [13].

MBMS streaming session: See TS 26.346: “Multimedia Broadcast/Multicast Service, Protocols and codecs” [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 MBMS service.

******* NEXT CHANGE *******

The following section shall be placed immediately before 4.2

4.x Granularity of MBMS security

An MBMS User Service is composed of one or more MBMS Streaming Sessions and/or MBMS Download Sessions as defined in TS 26.346 [13]. MBMS streaming/download sessions may be transported over one or more MBMS Transport Services. Transport Services are defined in [3]. MBMS security is used to protect MBMS streaming/download sessions. As such MBMS security is Transport Service independent, in particular, it is independent on whether it is carried over point-to-point or MBMS Bearer.

4.2 Key management overview

An MBMS User Service may use one or more MBMS Service Keys (MSKs), which may be in use at the same time and are managed at the MBMS User Service Level. The BM-SC controls the use of the MSKs to secure the different ~~Transport Service~~MBMS Streaming/Download Sessions that make up the MBMS User Service. The MSKs are not directly used to secure the MBMS ~~Transport Service~~MBMS Streaming/Download Sessions, but they are used to protect the delivery of MBMS Transport Keys (MTKs), which are used to secure the MBMS ~~Transport Service~~Streaming/Download Sessions, as specified within clauses 6.5 and 6.6.

NOTE: According to good security practice the use of the same MTK with two different security protocols shall be avoided.

For MBMS User Services it shall be possible to share one or more MSKs with other MBMS User Services, since according to TS 22.246 [5] there exist MBMS User Services with shared and non-shared Transport Services.

NOTE: While sharing MSKs among different MBMS User Services, care shall be taken that the Users are not given access to data that they are not entitled to.