3GPP TSG-SA-WG3 Meeting #33
10th – 14th May 2004, Beijing, China

Tdoc ⌘S3-0400229

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.246 CR CRNum** ⌘ **rev** ⌘ Current version: 1.1.0 ⌘

*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:	⌘	SRTP for streaming protection in MBMS
Source:	⌘	Ericsson
Work item code:	⌘	MBMS
Date:	⌘	05/04/2004
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:	⌘	MBMS Security protocol for streaming has not been specified
Summary of change:	⌘	SRTP is proposed
Consequences if not approved:	⌘	
Clauses affected:	⌘	2, 6.4

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

Other comments: ⌘

********FIRST CHANGE**********

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] IETF RFC 3711, Secure Real-time Transport Protocol

*********END OF FIRST CHANGE**********

********SECOND SET OF CHANGES**********

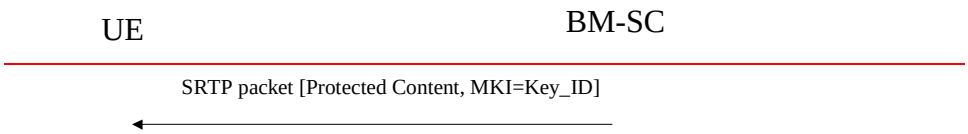
6.4 Protection of the transmitted traffic

The data transmitted to the UEs is protected by a symmetric key (an MTK) that is shared by the BM-SC and UEs that are accessing the MBMS service. The protection of the data is applied by the BM-SC. SRTP is used as security protocol for streaming MBMS data [6]. In order to determine which key was used to protect the data a Key_ID is included in the MKI (Master Key Identifier) field of SRTP packet. ~~with the protected data~~. The Key_ID will uniquely identify the MSK and contain other information needed to calculate the MTK. If the UE does not have the MSK indicated by Key_ID, then it should fetch the MSK using the methods discussed in the clause 6.2. The MTK is derived according to the methods described in clause 6.3.

Note: including the Key_ID with the protected data stops the UE trying to decrypt and render content for which it does not have the MSK.

Editor's note: The exact content of the Key_ID in the MKI field depends on the chosen key management solution.

The below flow shows how the protected content is delivered to the UE



After using a key to decrypt protected traffic, the UE deletes any older key for this multicast service.

Editor's note: this section may contain several protection methods.

Editor's note: if SRTP is chosen, the master key identifier can be used to indicate the current MBMS key whichever key management method is chosen