3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040620

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **1.2.1** ⌘

*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:	⌘	Combining S3-040552 and changes in clause 6.5 from S3-040573
Source:	⌘	MBMS Security Rapporteur
Work item code:	⌘	MBMS
Date:	⌘	09/07/2004
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:	⌘	To include the changes agreed in S3-040552 and S3-040573 in the MBMS TS.
Summary of change:	⌘	The agreed changes from S3-040552 and S3-040573 concerning SRTP and general and download protection requirements are combined into one CR
Consequences if not approved:	⌘	

Clauses affected:	⌘	2, 6.5

Other specs affected:	⌘	Y	N		⌘
			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: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[7] 3GPP TS 31.102: "T3-specification describing MBMS application and interface procedures on UICC"

[8] IETF RFC 2617 "HTTP Digest Authentication"

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

[10] "MIKEY: Multimedia Internet Keying", draft-ietf-msec-mikey-08.txt"

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

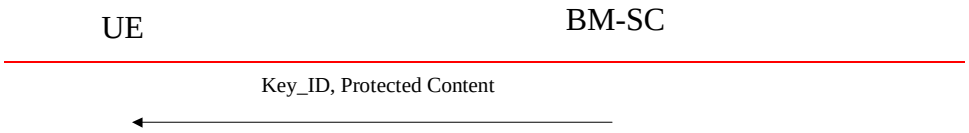
6.5 ~~6.5~~ Protection of the transmitted traffic

6.5.1 General

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. In order to determine which key was used to protect the data a Key_ID is included 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 6.3.~~ The MTK is derived according to the methods described in clause 6.4. Whenever data from an MBMS User Service has been decrypted, if it is to be stored on the UE it will be stored decrypted.

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.

~~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~~

6.5.2 Protection of streaming data

Editor's Note: The content of this clause will be checked after the joint meeting with SA4

6.5.2.1 Usage of SRTP

When it is required to protect MBMS streaming data SRTP (Secure Real-time Transport Protocol) as defined in [9] shall be used to protect MBMS streaming data. The MTK is carried to the UEs from the BM_SC using extended MIKEY. MTK shall be used as the master key in SRTP key derivation to derive the SRTP session keys as defined in chapter 4.3 of [9]. The correct MTK to use to decrypt the data is indicated using the MKI (Master Key identifier) field, which is included in the SRTP packets as defined in [9]. The form of MKI shall be a concatenation of MSK ID and MTK ID, i.e. MKI = (MSK ID || MTK ID).

If the SRTP packets are to be integrity protected, the SRTP authentication tag is appended to the packets as defined in [9].

SRTP security policy parameters, such as encryption algorithm, are transported in MIKEY Security Policy payload as defined in chapter 6.10.1 in [10].

6.5.1.2 Packet processing in the UE

When the SRTP module receives a packet, it will check if it has the MTK corresponding to the value in the MKI field in the cryptographic context.

NOTE: The SRTP module does not need to interpret the MKI field semantics. It only checks whether it has the MTK corresponding to the MKI value.

If the check is successful, the SRTP module processes the packet according to the security policy.

If the SRTP module does not have the MTK, it will request for MTK corresponding to the MKI from the key management module. When the key management module returns a new MTK, SRTP module will derive new session keys from the MTK and process the packet. However, if the key management module does not have the MSK indicated by MKI, then it should fetch the MSK using the methods discussed in the clause 6.3.

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

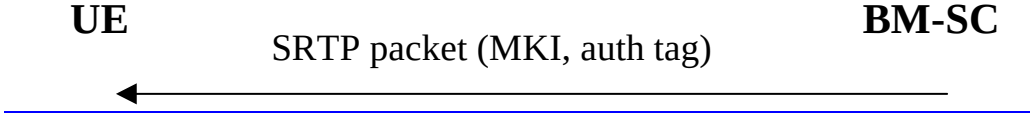


Figure x. Delivery of protected streaming content to the UE

6.5.3 Protection of download content

Data that belongs to a download MBMS User Service is decrypted as soon as possible by the UE, if the MSK needed to provide the relevant MTK is already available on the UE.