3GPP TSG SA WG3 Security — SA3#36 **S3-041018**

November 23 - 26, 2004

Shenzhen, China

Title: **CR corrections**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **MBMS**

1 Introduction

After SA3#35 it was found out that some of Ericsson's CRs were based on TS 33.246 v2.0.0 instead of v6.0.0. TS 33.246 v6.0.0 included some editorial modifications that were missing from v2.0.0.

The editorial modifications are mainly updating the RFC and TS references and using the work clause instead of clause. The only modifications that are not editorial are:

- Changes in 6.1 of S3-040850 are moved to 6.1 of S3-040887
- Deletion of a Note in 4.2 of S3-040850 is removed since the same text was changed in S3-040859
- Text "as is described in [6]" is moved from6.3.2.3.2 of S3-040850 to 6.3.2.2.4 S3-040889

Ericsson has now updated the approved Ericsson originated CRs from SA3#5 to be based on v6.0.0.The corrected versions are in the following list. The only one not Ericsson originated is S3-040887.

33.246	001	2	Rel-6	Deletion of MBMS keys stored in the ME	F	6.0.0	S3-35	S3-040863	MBMS	
33.246	002	-	Rel-6	Clarification on key management	C	6.0.0	S3-35	S3-040744	MBMS	
33.246	005	1	Rel-6	Clean up of MBMS TS	D	6.0.0	S3-35	S3-040850	MBMS	Replaced by CR_005_r2
33.246	006	1	Rel-6	Traffic protection combinations	F	6.0.0	S3-35	S3-040852	MBMS	
33.246	007	2	Rel-6	Clarifying ME and BM-SC capabilities	F	6.0.0	S3-35	S3-040887	MBMS	Replaced by CR_007_r3
33.246	008	1	Rel-6	MBMS Key processing	C	6.0.0	S3-35	S3-040858	MBMS	Replaced by CR_008_r2
33.246	009	1	Rel-6	MBMS MTK Download transport	C	6.0.0	S3-35	S3-040853	MBMS	
33.246	011	1	Rel-6	SRTP index synchronisation within ME	C	6.0.0	S3-35	S3-040854	MBMS	
33.246	013	1	Rel-6	Adding MIKEY payload type identifiers	F	6.0.0	S3-35	S3-040857	MBMS	Replaced by CR_013_r2

33.246	014	-	Rel-6	Protection of the Gmb reference point	C	6.0.0	S3-35	S3-040801	MBMS	
33.246	015	1	Rel-6	Use of parallel MSKs and MTKs	C	6.0.0	S3-35	S3-040859	MBMS	
33.246	016	1	Rel-6	Scope of MBMS security	C	6.0.0	S3-35	S3-040849	MBMS	Replaced by CR_016_r2
33.246	018	2	Rel-6	Clarification of the format of MTK ID and MSK ID	C	6.0.0	S3-35	S3-040888	MBMS	Replaced by CR_018_r3
33.246	020	1	Rel-6	MTK update procedure for streaming services	B	6.0.0	S3-35	S3-040855	MBMS	Replaced by CR_020_r2
33.246	021	2	Rel-6	Clarification of MSK key management	C	6.0.0	S3-35	S3-040889	MBMS	Replaced by CR_021_r3 This is submitted as a separate CR
33.246	022	1	Rel-6	Modification of delivery of MIKEY RAND field in MSK updates	C	6.0.0	S3-35	S3-040856	MBMS	

2 Conclusions and proposal

It is proposed that the updated versions are approved.

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

Tdoc ⌘Att1_S3-041018

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **005** ⌘**rev** **2** ⌘ 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⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Clean up of MBMS TS
Source:	⌘	Ericsson
Work item code:	⌘	MBMS
Date:	⌘	15/11/2004
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:

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:	⌘	Editorial clean up of MBMS TS
Summary of change:	⌘	Editorial clean up and editorial clarifications of MBMS TS
Consequences if not approved:	⌘	

Clauses affected:	⌘	Introduction, 1, 3.2, 3.3, 4.1, 5.3, 6.4.4, 6.4.6.1, 6.4.6.2, 6.5.4, 6.6.1

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

Other comments:	⌘	

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

Introduction

The security of MBMS provides different challenges compared to the security of services delivered over point-to-point services. In addition to the normal threat of eavesdropping, there is also the threat that it may not be assumed that valid subscribers have any interest in maintaining the privacy and confidentiality of the communications, and they may therefore conspire to circumvent the security solution (for example one subscriber may publish the decryption keys enabling non-subscribers to view broadcast content). Countering this threat requires the decryption keys to be updated frequently in a manner that may not be predicted by subscribers while making efficient use of the radio network.

1 Scope

The Technical Specification covers the security procedures of the Multimedia Broadcast/Multicast Service (MBMS) for 3GPP systems (UTRAN and GERAN). MBMS is a ~~GPRS~~ 3GPP system network bearer service over which many different applications could be carried. The actual method of protection may vary depending on the type of MBMS application.

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

3.2 Symbols

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

~~MUK_I Integrity key derived from key MUK~~
~~MUK_C Confidentiality key derived from key MUK~~
~~MSK_I Integrity key derived from key MSK~~
~~MSK_C Confidentiality key derived from key MSK~~

3.3 Abbreviations

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

MBMS Multimedia Broadcast/Multicast Service
MGV-F MBMS key Generation and Validation Function
MGV-S MBMS key Generation and Validation Storage
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

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

4.1 MBMS security architecture

MBMS introduces the concept of a point-to-multipoint service into a 3GPP system. A requirement of a multicast service is to be able to securely transmit data to a given set of users. In order to achieve this, there needs to be a method of authentication, key distribution and data protection for a multicast service. ~~The AKA protocol (see TS 33.102 [4]) is~~

~~used to both authenticate a user and agree on keys to be used between that user and the network. These keys are subsequently used to provide protection of traffic between the network and the UE.~~

Figure 4.1: MBMS security architecture

Figure 4.1 gives an overview of the network elements involved in MBMS from a security perspective. Nearly all the security functionality for MBMS (beyond the normal network bearer security) resides in either the BM-SC or the UE.

The Broadcast Multicast – Service Centre (BM-SC) is a source for MBMS data. It could also be responsible for scheduling data and receiving data from third parties (this is beyond the scope of the standardisation work) for transmission. It is responsible for generating and distributing the keys necessary for multicast security to the UEs and for applying the appropriate protection to data that is transmitted as part of a multicast service. The BM-SC also provides the MBMS bearer authorisation for UEs attempting to establish multicast bearer.

The UE is responsible for receiving or fetching keys for the multicast service from the BM-SC and also using those keys to decrypt the MBMS data that is received.

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

5.3 Protection of the transmitted traffic

The traffic for a particular MBMS service may require some protection depending on the sensitivity of the data being transmitted (e.g. it is possible that the data being transmitted by the MBMS service is actually protected by the DRM security method and hence might not require~~s no~~ additional protection. However, MBMS protection is independent of DRM protection). This protection will be either confidentiality and integrity or just confidentiality. The protection is applied end-to-end between the BM-SC and the UEs and will be based on a symmetric key shared between the BM-SC and the UEs that are currently accessing the service. The actual method of protection specified may vary depending on the type of data being transmitted, e.g. media streaming application or file download.

NOTE: When MBMS data is received over a point-to-point MBMS radio bearer, it would be ciphered between the BM-SC and UE and may also ciphered over the radio interface. This “double ciphering” is unnecessary from a security point of view and hence the decision of whether or not to apply radio interface ciphering to a point-to-point MBMS radio bearer is outside the scope of this specification.

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

6.4.4 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in RFC 3830 [9] (MIKEY). To be able to keep track of the keys, a new general Extension Payload (EXT) is defined that conforms to the structure defined in section 6.15 of RFC 3830 [9] (MIKEY). The IDs of the involved keys are kept in the EXT, to enable the UE to look up the identity of the key which was used to protect the message, and which key is delivered in the message. This EXT is incorporated in the MIKEY messages (see Figure 6.4). When an MSK is delivered to a UE, the MIKEY message contains an EXT that holds the MUK ID of the MUK used to protect the delivery, and the MSK ID of the MSK delivered in the message. For messages that contain an MTK, the EXT contains the MSK ID of the MSK used to protect the delivery, and the MTK ID of the MTK contained in the message. The MSK ID and MTK ID are increased by 1 every time the corresponding key is updated. It is possible that the same MTK is delivered several times in multicast, and the ME can then discard messages related to a key it already has instead of passing them to the MGV-F.

The MGV-F (see clause 6.5) protects itself from a possibly malicious ME by checking the integrity and freshness of the MIKEY message.

The format of the key IDs shall be represented by unsigned integer counters, different from zero. The reason for disallowing zero is that it is reserved for future use. Note that this means that there can only be ~~2^{n} - 1~~ $2^n - 1$ different keys in use during the same session, where n is the number of bits in the ID field.

Outer Key ID	Inner Key ID

Figure 6.4: Extension payload used with MIKEY

The Inner Key ID is the ID of the key that is transported in the message (i.e. an MSK or MTK). The Outer Key ID is the ID of the key used as pre-shared secret for the key delivery (i.e. an MUK or MSK).

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

6.4.6.1 MSK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of RFC 3830 [9]).

1. The Data Type field of the common MIKEY header (HDR) is examined, and if it indicates an MSK delivery, the MUK ID is extracted from the Extension Payload.
2. The Timestamp Payload is checked, and the message is discarded if the counter in the Timestamp Payload is ~~larger~~ smaller or equal to the ~~current MIKEY~~ stored replay counter associated with the given MUK (the stored replay counter value is retrieved from MGV-S). To avoid issues with wrap around of the ID fields ``smaller than´´ should be in the sense of RFC1982 [10].
3. The Security Policy payload is stored if it was present.
4. The message is transported to MGV-F for further processing, cf 6.5.2.
5. The MGV-F replies success or failure.

6.4.6.2 MTK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of RFC 3830 [9]).

1. The Data Type field of the common MIKEY header (HDR) is examined, and if it indicates an MTSK delivery, the MSK ID is extracted from the Extension Payload.
2. The Timestamp Payload is checked, and the message is discarded if the counter in the Timestamp Payload is ~~larger~~ smaller or equal to the ~~current MIKEY~~stored replay counter associated with the given MSK (the stored replay counter value is retrieved from MGV-S). To avoid issues with wrap around of the ID fields ``smaller than´´ should be in the sense of RFC1982 [10].
3. If the MTK ID extracted from the Extension payload is less than or equal to the current MTK ID (kept in the ME), the message shall be discarded.
4. The message is transported to MGV-F for further processing, cf 6.5.3.
5. The MGV-F replies success (i.e. sending the MTK) or failure.

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

6.5.4 MTK validation and derivation

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the Data Type field in the common header. If the key inside the message is an MTK, MGV-F retrieves the MSK with the ID given by the Extension payload.

It is assumed that the MBMS service specific data, MSK and the sequence number SEQs, have been stored within a secure storage (MGV-S). Both MSK and SEQs were transferred to the MGV-S with the execution of the MSK update procedures. The initial value of SEQs is determined by the service provider.

The MGV-F shall only calculate and deliver the MBMS Traffic Keys (MTK) to the ME if the ptm-key information is deemed to be fresh.

The MGV-F shall compare the received SEQp, i.e. MTK ID from the MIKEY message with the stored SEQs. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME. If SEQp is greater than SEQs then the MGV-F shall calculate the MAC as defined in RFC 3830 [9] using the received MIKEY message and MSK as input. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message. If the MAC verification is unsuccessful, then the MGV-F will indicate a failure to the ME. If the MAC verification is successful, then the MGV-F shall update SEQs with SEQp value and start the generation of MTK. The MGV-F provides the MTK to the ME.

If MAC verification is successful, ~~T~~the MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MSK ID.

NOTE: MIKEY includes functionality to derive further keys from MTK if needed by the security protocol. The key derivation is defined in section 4.1.3 of RFC 3830 [9] (MIKEY).

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

6.6.1 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 key identification information is included with the protected data. The key identification information ~~Key_ID~~ will uniquely identify the MSK and ~~contain other information needed to calculate the~~ MTK. The MTK is ~~derived~~ processed according to the methods described in subclauses 6.4 and 6.5. 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 identification information with the protected data stops the UE trying to decrypt and render content for which it does not have the MSK.

3GPP TSG-SA WG3 Meeting S3#36
Shenzhen, China, November 23-26, 2004

Tdoc ⌘Att2_S3-041018

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **007** ⌘**rev** **4** ⌘ 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⌘ ☐ ME [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	Clarifying ME and BM-SC capabilities
Source:	⌘	Ericsson
Work item code:	⌘	MBMS
Date:	⌘	15/11/2004
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:	⌘	The specification is not entirely clear that the ME shall support key management functions and the BM-SC shall support using GBA_U keys. Furthermore the text stating what shall be supported by an ME and UICC is in a clause about using GBA for MBMS which is not really the best place for this text. The text is moved to an overview clause where it fits better.
Summary of change:	⌘	The text stating what an MBMS capable ME and UICC shall support is moved to a more appropriate clause. Text is added to clarify that an ME shall support ME key management and the BM-SC supports using GBA_U keys.
Consequences if not approved:	⌘	The specification is not clear on the ME supporting MBMS key management and the BM-SC supporting GBA_U keys.

Clauses affected:	⌘	4.1, 6.1
Other specs affected:	⌘	Y N ☐ N Other core specifications ☐ N Test specifications ☐ N O&M Specifications
Other comments:	⌘	

********** First Modification **********

4.1 MBMS security architecture

MBMS introduces the concept of a point-to-multipoint service into a 3GPP system. A requirement of a multicast service is to be able to securely transmit data to a given set of users. In order to achieve this, there needs to be a method of authentication, key distribution and data protection for a multicast service. The AKA protocol (see TS 33.102 [4]) is used to both authenticate a user and agree on keys to be used between that user and the network. These keys are subsequently used to provide protection of traffic between the network and the UE.

Figure 4.1: MBMS security architecture

Figure 4.1 gives an overview of the network elements involved in MBMS from a security perspective. Nearly all the security functionality for MBMS (beyond the normal network bearer security) resides in either the BM-SC or the UE.

The Broadcast Multicast – Service Centre (BM-SC) is a source for MBMS data. It could also be responsible for scheduling data and receiving data from third parties (this is beyond the scope of the standardisation work) for transmission. It is responsible for generating and distributing the keys necessary for multicast security to the UEs and for applying the appropriate protection to data that is transmitted as part of a multicast service. The BM-SC also provides the MBMS bearer authorisation for UEs attempting to establish multicast bearer.

The UE is responsible for receiving or fetching keys for the multicast service from the BM-SC and also using those keys to decrypt the MBMS data that is received.

MBMS imposes the following requirements on the MBMS capable elements:

- a UICC that contains MBMS key management functions shall implement GBA_U;
- a ME that supports MBMS shall implement GBA_U and GBA_ME, and shall be capable of utilising the MBMS key management functions on the UICC as well as providing key management functions itself;
- a BM-SC shall support using GBA_U keys to enable UICC key management.

********** Next Modification **********

6.1 Using GBA for MBMS

TS 33.220 [6] (Generic Bootstrapping Architecture) is used to agree keys that are needed to run an MBMS Multicast User service. ~~MBMS imposes the following requirements on the MBMS capable UICCs and MEs:~~

- ~~a UICC that contains MBMS key management functions shall implement GBA_U;~~
- ~~a ME that supports MBMS shall implement GBA_U and GBA_ME, and shall be capable of utilising the MBMS key management functions on the UICC.~~

Before a user can access an MBMS User service, the UE needs to share GBA-keys with the BM-SC. If no valid GBA-keys are available at the UE, the UE shall perform a GBA run with the BSF of the home network as described within clause 5 of TS 33.220 [6]. The BM-SC will act as a NAF (Network Application Function) according to TS 33.220 [6].

The MSKs for an MBMS User service shall be stored on either the UICC or the ME. Storing the MSKs on the UICC requires a UICC that contains the MBMS management functions (and that is GBA aware) and requires that the BM-SC is GBA_U aware. As a result of the GBA_U run in these circumstances, the BM-SC will share a key Ks_ext_NAF with the ME and share a key Ks_int_NAF with the UICC. This key Ks_int_NAF is used by the BM-SC and the UICC as the key MUK (MBMS User Key) to protect MSK (MBMS Service Key) deliveries to the UICC as described within

clause 6.3. The key Ks_ext_NAF is used as the key MRK(MBMS Request Key) within the protocols as described within clause 6.2.

NOTE: A run of GBA_U on a GBA aware UICC will not allow the MSKs to be stored on the UICC, if the MBMS management functions are not present on the UICC.

In any other circumstance, a run of GBA results in the BM-SC sharing a key Ks_(ext)_NAF with the ME. This key Ks_(ext)_NAF is used by the BM-SC and the ME to derive the key MUK and the key MRK ~~(MBMS Request Key)~~. The key MUK is used to protect MSK deliveries to the ME as described within clause 6.3. The key MRK is used to authenticate the UE towards the BM-SC within the protocols as described within clause 6.2.

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

Tdoc ⌘Att3_S3-041018

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **008** ⌘**rev** **2** ⌘ 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:	⌘	MBMS Key processing
Source:	⌘	Ericsson
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:	⌘	Processing of MTKs and MSKs needed clearification
Summary of change:	⌘	• Moved text from 6.4.2 to 6.4.1, since this text is more general than the heading suggests. • Changed Sections 6.5.3 and 6.5.4, so that they now refer to the MIKEY specification instead of re-stating the same functionality again. Having the functionallity specified in two places only creates confusion. Especially, the change implies that MIKEY's built in PRF is used for key derivation. This should be prefered, since introducing a new PRF requires time consuming analysis to determine that the new PRF is secure in the new setting.
Consequences if not approved:	⌘	The usage of MTK and MSK will be underspecified.

Clauses affected:	⌘	6.4.1, 6.4.2, 6.5.2, 6.5.3, 6.5.4

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

Other comments:	⌘	

__FIRST_CHANGE__

6.4 MIKEY message creation and processing in the ME

Editor's note: The need for salting keys in processing of MIKEY messages is for further study.

6.4.1 General

MIKEY is used to transport the MSKs and MTKs from the BM-SC to the UE. Clauses 6.4.2, 6.4.3, 6.4.4 and 6.4.5 describe how to create the MIKEY messages, while clause 6.4.6 describes the initial processing by the ME on these messages. The final processing is done by the MBMS key Generation and Validation Function (MGV-F) and is described in clause 6.5.

MIKEY shall be used with pre-shared keys as described in RFC 3830 [9].

To keep track of MSKs and MTKs, a new Extension Payload (EXT) is added to MIKEY. The Extension contains the identities of MSKs and the MTKs (see clause 6.3.2 and 6.3.3).

6.4.2 MIKEY common header

~~MIKEY shall be used with pre-shared keys as described in RFC 3830 [9].~~

MSKs shall be carried in MIKEY messages with a Data Type value of 0x07 in the MIKEY common header that signals that the message contains an MBMS MSK. This allows legacy MIKEY implementations to discard the message early in the processing stage. The messages are sent point-to-point between the BM-SC and each UE. The messages use the MUK shared between the BM-SC and the UE as the pre-shared secret in MIKEY.

Once the MSK is in place in the UE, the UE can make use of the multicast MTK messages sent by the BM-SC. The MTK is carried in messages conforming to the structure defined by MIKEY and use the MSK as the pre-shared secret. A Data Type value of 0x08 is used in the MIKEY common header to signal that the message contains an MBMS MTK.

~~To keep track of MSKs and MTKs, a new Extension Payload (EXT) is added to MIKEY. The Extension contains the identities of MSKs and the MTKs (see clause 6.3.2 and 6.3.3).~~

If the BM-SC requires an ACK for an MSK key update message this is indicated by setting the V-bit in the MIKEY common header. The UE shall then respond with a MIKEY message containing the verification payload. In the case the server does not receive an ACK, normal reliability constructions can be used, e.g., start a timer when the message is sent and then resend the message if no ACK is received before the timer expires.

The CSB ID field of MIKEY common header shall carry the Key Group ID.

__SECOND_CHANGE__

6.5.2 MUK derivation

When a MUK has been installed in the MGV-S, i.e. as a result of a GBA run, it is used as pre-shared secret ~~together with the MIKEY_RAND and the Key Group ID from the MIKEY message to derive encryption and integrity keys (MUK_C and MUK_I) as defined in section 4.1.4 of MIKEY. MUK_I and MUK_C are~~ used to verify the integrity of the MSK transport message and decrypt the key carried in the KEMAC payload as described in RFC 3830 [9].

6.5.3 MSK processing~~validation and derivation~~

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the Data Type field in the common header. If the key in the message is an MSK, MGV-F retrieves the MUK with the ID given by the Extension payload.

~~The MAC in the KEMAC payload is verified using MUK_I, and the message is discarded if verification fails. If the MAC verification is successful the MUK_C is used to decrypt the Key Data sub-payload, and the MSK can be installed in the MGV-S. The MSK is used as pre-shared secret together with the MIKEY-RAND and the Key Group ID from the MIKEY message to derive (as specified in section 4.1.4 of RFC 3830 [9]) encryption and integrity keys (MSK_I and MSK_C).~~ The integrity of the message is validated and the MSK is extracted from the KEMAC payload as described in Section 5 of [9] if the validation is successful. The Key Validity data is extracted from the message and stored (in the form of MTK ID interval). The lower limit of the interval defines the SEQs.

NOTE: The MSK is not necessarily updated in the message, since a MSK transport message can be sent e.g. to update the Key Validity data.

If message~~MAC verific~~validation is successful, then the MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MUK ID.

6.5.4 MTK processing~~validation and derivation~~

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the Data Type field in the common header. If the key inside the message is an MTK, MGV-F retrieves the MSK with the ID given by the Extension payload.

It is assumed that the MBMS service specific data, MSK and the sequence number SEQs, have been stored within a secure storage (MGV-S). Both MSK and SEQs were transferred to the MGV-S with the execution of the MSK update procedures. The initial value of SEQs is determined by the service provider.

The MGV-F shall only calculate and deliver the MBMS Traffic Keys (MTK) to the ME if the ptm-key information is deemed to be fresh.

The MGV-F shall compare the received SEQp, i.e. MTK ID from the MIKEY message with the stored SEQs. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME. If SEQp is greater than SEQs then the MGV-F shall verify the integrity of the MIKEY message according to RFC 3830 [9]. ~~calculate the MAC as defined in RFC 3830 [9] using the received MIKEY message and MSK as input. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message~~. If the ~~MAC~~ verification is unsuccessful, then the MGV-F will indicate a failure to the ME. If the ~~MAC~~ verification is successful, then the MGV-F shall update SEQs with SEQp value and extract the ~~start the generation of~~ MTK from the message. The MGV-F then provides the MTK to the ME.

The MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MSK ID.

NOTE: MIKEY includes functionality to derive further keys from MTK if needed by the security protocol. The key derivation is defined in section 4.1.3 of RFC 3830 [9] (MIKEY).].

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

Tdoc ⌘Att4_S3-041018

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **016** ⌘**rev** **2** ⌘ 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:	⌘	Ericsson
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.

3GPP TSG-SA3 Meeting #35
Shenzen, China, 23-26 November, 2004

Tdoc ⌘Att5_S3-041018

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **018** ⌘**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:	⌘	Clarification of the format of MTK ID and MSK ID.
Source:	⌘	Ericsson
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 format of MSK ID and MTK ID is unclear. According to the TS MTK ID is a sequence number while MSK ID is not.
Summary of change:	⌘	The format of MSK ID and MTK ID are clarified. MSK ID is not a sequence number. MTK ID is a sequence number with length of 2 bytes and it shall be increased by 1 modulo 2exp<key id length in bits>, when MTK is updated.
Consequences if not approved:	⌘	MSK IDs and MTK IDs remains unclear.

Clauses affected:	⌘	6.3.3.1, 6.4.4

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

Other comments:	⌘	

6.3.3.1 MTK identification

Every MTK is uniquely identifiable by its Network ID, Key Group ID, MSK ID and MTK ID

where

Network ID, Key Group ID and MSK ID are as defined in clause 6.3.2.1.

MTK ID is 2 bytes long sequence number and is used to distinguish MTKs that have the same Network ID, Key Group ID and MSK ID. It is carried in the MTK-ID field of MIKEY extension payload. The MTK ID shall be increased by 1 modulo 2 (MTK ID length in bits) every time the MTK is updated. The MTK ID shall be reset every time the MSK is updated.

~~Editor's Note: The format of MTK is ffs.~~

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

6.4.4 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in RFC 3830 [9] (MIKEY). To be able to keep track of the keys, a new general Extension Payload (EXT) is defined that conforms to the structure defined in 6.15 of RFC 3830 [9] (MIKEY). The IDs of the involved keys are kept in the EXT, to enable the UE to look up the identity of the key which was used to protect the message, and which key is delivered in the message. This EXT is incorporated in the MIKEY messages (see Figure 6.4). When an MSK is delivered to a UE, the MIKEY message contains an EXT that holds the MUK ID of the MUK used to protect the delivery, and the MSK ID of the MSK delivered in the message. For messages that contain an MTK, the EXT contains the MSK ID of the MSK used to protect the delivery, and the MTK ID of the MTK contained in the message. Cf. subclauses 6.3.2.1 and 6.3.3.1 for definition of MSK ID and MTK ID. The ~~MSK ID and~~ MTK ID ~~are~~ is increased by 1 modulo 2 (key ID length in bits) every time the corresponding key is updated. It is possible that the same MTK is delivered several times in multicast, and the ME can then discard messages related to a key it already has instead of passing them to the MGV-F.

The MGV-F (see clause 6.5) protects itself from a possibly malicious ME by checking the integrity and freshness of the MIKEY message.

The format of the key IDs shall be represented by unsigned integers ~~counters~~, different from zero. The reason for disallowing zero is that it is reserved for future use. Note that this means that there can only be 2^{n} - 1 different keys in use during the same session, where n is the number of bits in the ID field.

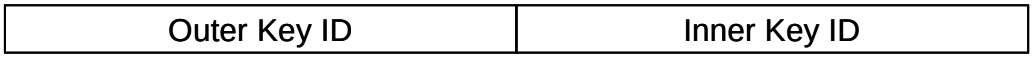


Figure 6.4: Extension payload used with MIKEY

The Inner Key ID is the ID of the key that is transported in the message (i.e. an MSK or MTK). The Outer Key ID is the ID of the key used as pre-shared secret for the key delivery (i.e. an MUK or MSK).

3GPP TSG-SA WG3 Meeting S3#36
Shenzen, China, 23-26 November, 2004

Tdoc ⌘Att6_S3-041018

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **020** ⌘**rev** **2** ⌘ 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⌘ ☐ ME [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	MTK update procedure for streaming services
Source:	⌘	Ericsson
Work item code:	⌘	MBMS
Date:	⌘	15/11/2004
Category:	⌘	**B**
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:	⌘	It is not specified how the MTK is transported to the UE in streaming services
Summary of change:	⌘	MTK is interleaved with the RTP traffic and separated with UDP port number
Consequences if not approved:	⌘	It will remain unspecified how the MTK is delivered in streaming services.

Clauses affected:	⌘	6.3.3.2, 6.3.3.2.2 (new), 6.6.2.2

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

Other comments: ⌘

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

6.3.3.2 MTK update procedures

The MTK is delivered to the UE as in 6.3.2.3.1 but the MIKEY ACK is not used.

6.3.3.2.2 MTK delivery in streaming

MIKEY messages transporting MTKs shall be sent using the same IP address as the RTP traffic. MIKEY messages shall be transported to UDP port number specified for MIKEY.

Editor's Note: The UDP port number needs to be specified for MIKEY.

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

6.6.2 Protection of streaming data

6.6.2.1 Usage of SRTP

When it is required to protect MBMS streaming data SRTP (Secure Real-time Transport Protocol) as defined in RFC 3711 [11] shall be used. The MTK is carried to the UEs from the BM-SC using RFC 3830 [9] (MIKEY) with extensions defined according to this specification. MTK shall be used as the master key in SRTP key derivation to derive the SRTP session keys as defined in section 4.3 of RFC 3830 [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 RFC 3711 [11]. The form of MKI shall be a concatenation of Network ID, Key Group ID, MSK ID and MTK ID, i.e. MKI = (Network ID || Key Group ID || 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 RFC 3830 [9].

SRTP security policy parameters, such as encryption algorithm, are transported in MIKEY Security Policy payload as defined in section 6.10.1 in RFC 3830 [9].

6.6.2.2 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 SRTP 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 the MTK corresponding to the MKI from the key management module. When the key management module returns a new MTK, the 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.

If the correct MTK is not present in the UE when RTP traffic arrives, the UE shall wait for the next MTK update procedure from the BM-SC as described in 6.3.3.2.

NOTE: It is implementation specific issue whether the UE spools encrypted packets or discards all packets before the UE has received the correct MTK.

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

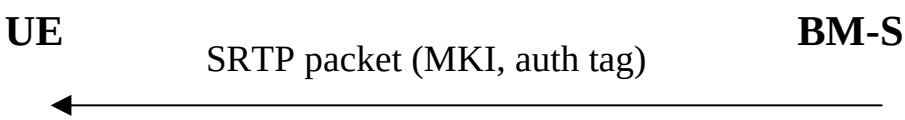


Figure 6.8: Delivery of protected streaming content to the UE

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

Tdoc ⌘Att7_S3-041018

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **021** ⌘ **rev** **5** ⌘ 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⌘ ☐ ME [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	Clarification of MSK key management
Source:	⌘	Ericsson
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:	⌘	Initiation of key management is not specified. The details of MSK request from UE to the BM-SC are unclear. The details of MIKEY solicit message from the BM-SC are unclear. The structure of the MSK procedure sections are enhanced. The split to pull and push procedures is seen to be more clear and enable smoother update of the TS in the future, if for example new triggers are introduced for pulling the MSK from the BM-SC like initiation of key management
Summary of change:	⌘	Initiation of key management is specified. Required Security parameters in Service Annoucement are specified. It is specified that the UE shall request for the Key Group ID(s) from the BM-SC. MSK ID(s) are not needed in the request since BM-SC will send the current valid MSK for each Key Group ID. BM-SC should solicit the UE to contact the BM-SC by setting the MSK ID to 0x0 in the MIKEY MSK message. The message will not carry any MSK.
Consequences if not approved:	⌘	Initiation and details of MBMS key management messages remain unspecified.

Clauses affected:	⌘	2, 6.3.2.2, 6.3.2.2.1 (new), 6.3.2.2.2 (new), 6.3.2.2.3 (new), 6.3.2.2.4 (new), 6.3.2.3, 6.3.2.3.2 (void)

	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] 3GPP TS 26.346: "MBMS, Protocols and codecs".

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

6.3.2 MSK procedures

6.3.2.1 MSK identification

Every MSK is uniquely identifiable by its Network ID, Key Group ID and MSK ID

where

Network ID = MCC || MNC and is 3 bytes long. It is carried in the IDi payload in MIKEY message

Key Group ID is 2 bytes long and is used to group keys together in order to allow redundant MSKs to be deleted. It is carried in the CSB ID field of MIKEY common header.

MSK ID is 2 bytes long and is used to distinguish MSKs that have the same Network ID and Key Group ID. It is carried in the MSK-ID field of MIKEY extension payload.

If the UE receives an MSK and already contains two other MSKs under the same Network ID and Key Group ID, then the UE shall delete the older of these two MSKs.

Editor's Note: The handling of MSKs may need some enhancement to cover download services, where the MSK is fetched after the UE has received the encrypted data.

6.3.2.2 ~~UE initiated~~ MSK retrieval ~~update~~ procedures

6.3.2.2.1 Basic MSK retrieval procedure

When a UE detects that it needs the MSK(s) for a specific MBMS User service, the UE should try to get the MSK(s) that will be used to protect the data transmitted as part of this ~~multicast~~ User ~~s~~Service. In the MSK request the UE shall list the Key Group IDs for which the UE needs the MSK(s).

The basic MSK retrieval procedure is a part of different other procedures, e.g.~~Reasons for UE to retrieve the MSK(s) include e.g.:~~

- ~~retrieval of initial MSKs~~ initiation of key management ~~e.g.~~ when the UE has joined the MBMS user service;

~~Editor's note: The initial key request may also be part of User Service joining procedure if SA4 decides to have such procedure. In this case the MSKs will be transported after the joining procedure has completed.~~

- ~~—~~retrieval of MSK(s) when the UE has missed a key update procedure e.g. due to being out of coverage~~.~~

- BM-SC solicited pull~~If the UE fails to get hold of the MSK or receives confirmation that no updated MSK is necessary or available at this time, then, unless the UE has a still valid, older MSK, the UE shall leave the MBMS user service~~

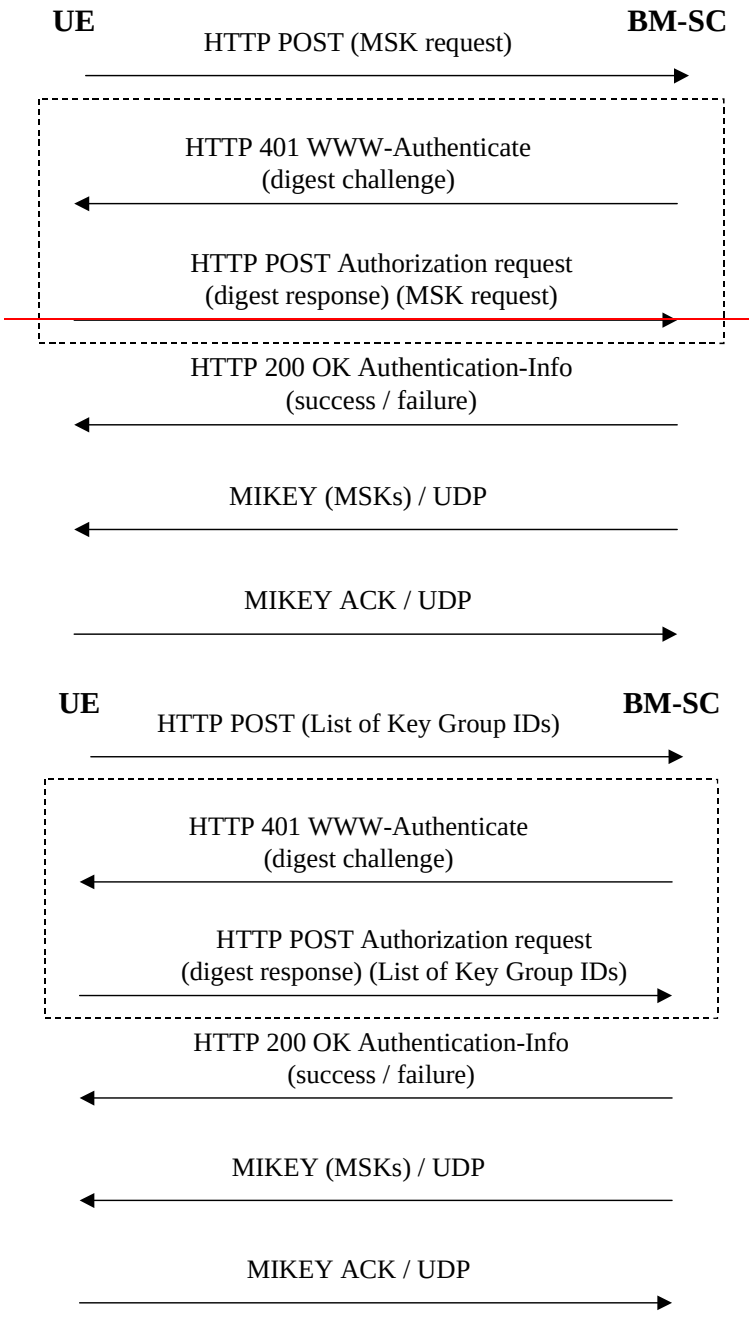


Figure 6.1: ~~UE initiated MSK delivery~~Basic MSK retrieval procedure

The communication between the UE and the BM-SC is authenticated and integrity protected with HTTP Digest as described in subclause 6.2.1 of this specification.

The UE requests for the MSKs ~~using~~ with ~~the~~ HTTP POST message. The following information ~~key identification information~~ is included in the ~~client payload of the~~ HTTP message

- key identification information: a list of Key Group IDs~~.~~

NOTE: MSK ID(s) are not needed in the request since BM-SC will send the current valid MSK for each Key Group ID.

Editors' Note: The exact syntax of the HTTP request message, e.g. possible XML schema of the request parameters in the client payload and its MIME type are to be specified in stage 3.

The BM-SC authenticates the UE with HTTP Digest using the keys received from GBA as described in subclause 6.2.1 and verifies that the subscriber is authorized to receive the MSKs for this service. ~~may challenge the UE with HTTP response including WWW-Authenticate header and digest-challenge. Upon receiving the digest-challenge, the UE~~

~~calculates the digest response and re-sends HTTP POST message including the key request and Authorization Request header including the digest response.~~

The BM-SC sends a response in HTTP 200 OK message with Authentication-Info header. The response ~~in client payload~~ includes ~~cause code for~~ success or ~~reject~~failure.

Editors' Note: The exact syntax of the HTTP response message, e.g. possible XML schema of the success or failure parameters in the client payload and its MIME type are to be specified in stage 3.

The UE checks the validity of the HTTP response message. If the message indicated failure, the UE may retry or leave the User Service.

If the ~~key request~~HTTP procedure above resulted to success, the BM-SC ~~sends~~ initiates MIKEY message~~s~~ procedures over UDP transporting the requested MSKs to the UE.

If it was requested by the BM-SC, the UE sends a MIKEY acknowledgement message to the BM-SC.

If the UE fails to get hold of the MSK or receives no confirmation that no updated MSK is necessary or available at this time, then, unless the UE has a still-valid, older MSK, the UE shall leave the MBMS user service.

6.3.2.2.2 Initiation of key management

When a UE has received User Service information via User Service Discovery / Announcement procedures describing a MBMS User Service and the user has triggered the activation of that User Service, the UE should try to get the MSK(s) that will be used to protect the data transmitted as part of this User Service.

NOTE: The User Service Discovery / Announcement procedures are specified in TS 26.346 [13]. It is out of the scope of the present specification how the UE receives the User Service information and how the User Service is triggered in the UE.

The UE shall receive the following information via the User Service Discovery / Announcement procedures:

- Domain name of the key management server (i.e. the BM-SC). This for the UE to know to which IP address to send the MSK request
- Confidentiality protection: on / off
- Integrity protection: on / off
- Identifiers of the Key Groups IDs needed for the User Service

NOTE: MSK ID(s) are not used since they may change over time and Key Group ID is sufficient to identify the MSKs.

- Mapping information how the MSKs are used to protect the different User Service Sessions

Editors' Note: The exact syntax of the service announcement information including security parameters, e.g. possible XML schema of the parameters and its MIME type are to be specified in SA4.

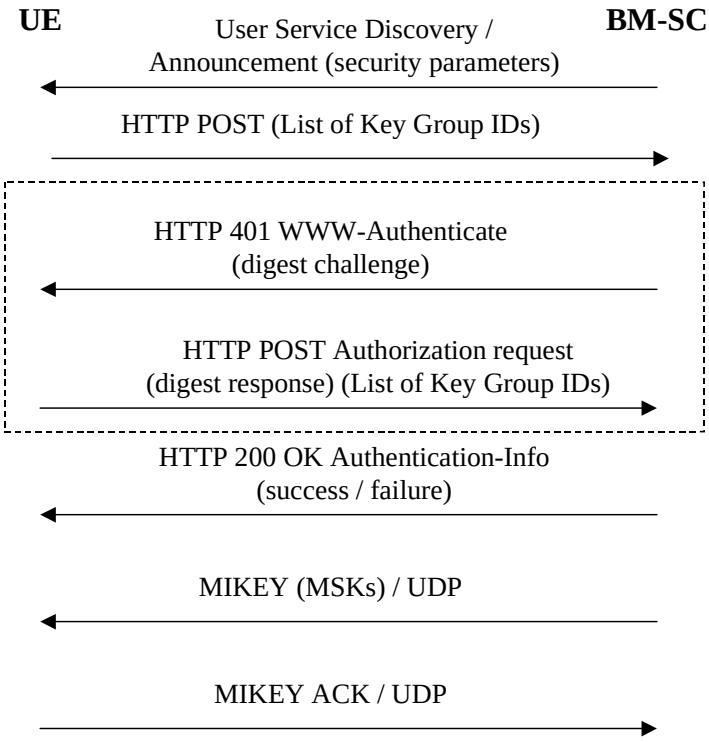


Figure 6.x: MSK retrieval procedure

The communication between the UE and the BM-SC is authenticated and integrity protected with HTTP Digest as described in subclause 6.2.1 of this specification.

The UE requests for the MSKs using with the HTTP POST message.

The rest of the procedure is the same as in 6.3.2.3.1.

6.3.2.2.3 Missed key update procedure

When the UE has missed an MSK update and it detects that it has not got the current MSK, e.g. from the received traffic, it may trigger the retrieval of the current MSK from the BM-SC. The procedure is the same as the Basic MSK Retrieval procedure in subclause 6.3.2.3.1.

6.3.2.2.4 BM-SC solicited pull

While the push is the regular way of updating the MSK to the UE, there may be situations where the BM-SC solicits the UE to contact the BM-SC and request for new MSK. Examples of such situations are when the BM-SC wants the UE to authenticate itself during the service or when the MUK has expired or when the BM-SC wants to re-key all UEs.

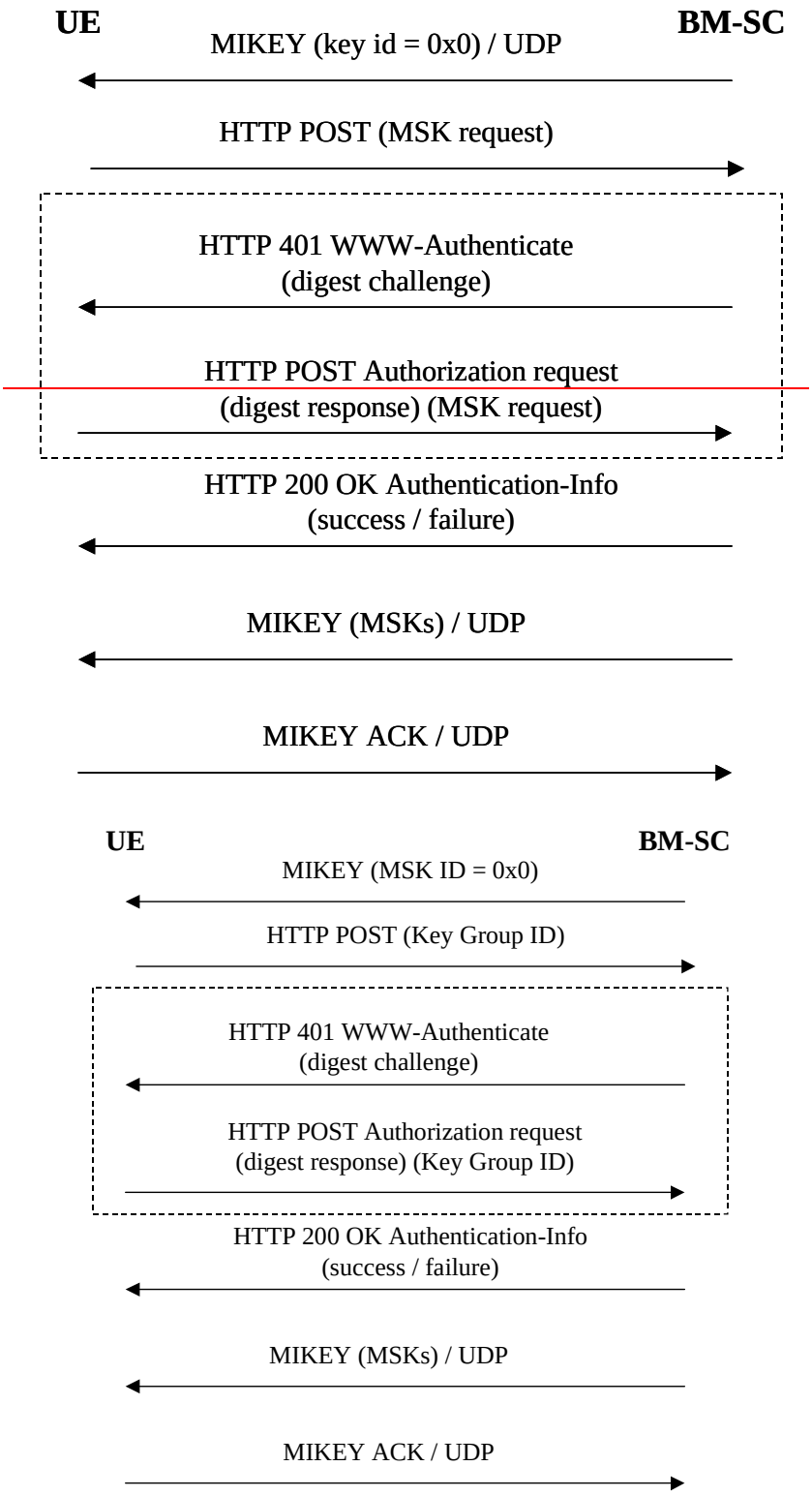


Figure 6.3: BM-SC solicited pull

The BM-SC sends MIKEY message over UDP to the UE. The MSK ID in the extension payload of the MIKEY message shall be set to 0x0 to indicate that the UE should request for current MSK from the BM-SC.

NOTE: Since the integrity of the MIKEY message still needs to be assured, a KEMAC payload shall be included in the MIKEY message from the BM-SC. There is however no key present in the message. Thus by setting the Encr data len field to zero, only the MAC of the message will be included.

When receiving the message, the UE shall request for the MSK for the specified Key Group. The BM-SC may trigger re-authentication of the UE or even re-run of GBA procedure to update the MUK as is described in [6].

The rest of the procedure is the same as in 6.3.2.3.1.

6.3.2.3 ~~BM-SC initiated~~ MSK ~~update~~ push procedures

6.3.2.3.1 Pushing the MSKs to the UE

The BM-SC controls when the MSKs used in a multicast service are to be changed. The below flow describes how MSK changes are performed.

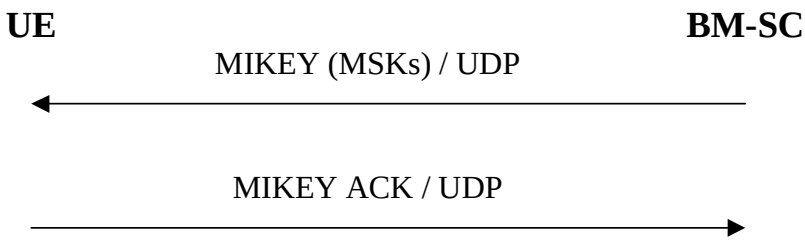


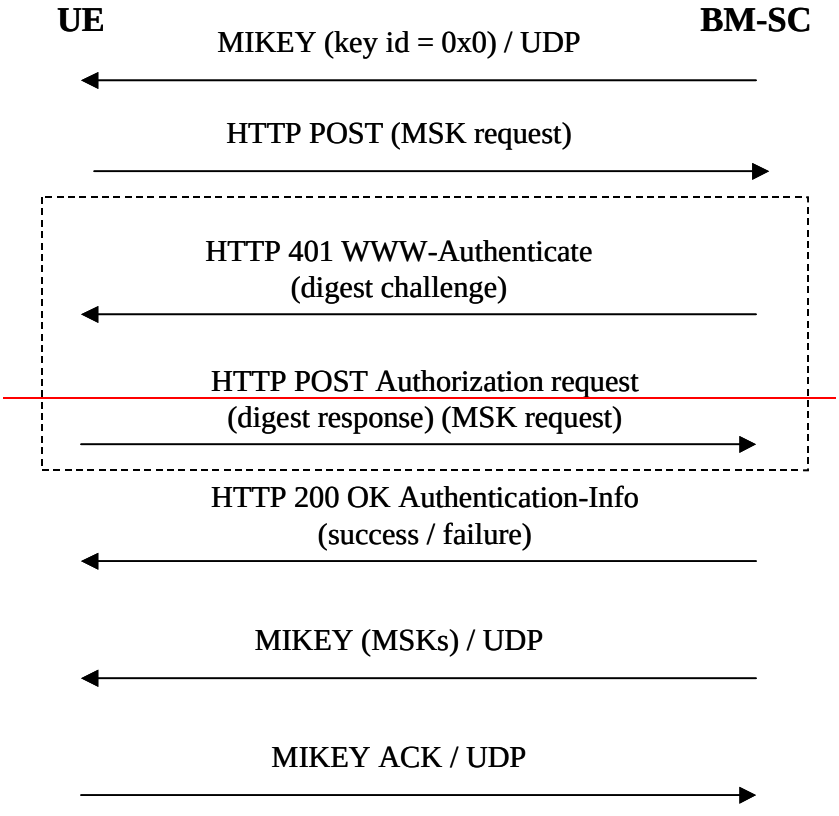
Figure 6.2: Pushing the MSKs to the UE

When the BM-SC decides that it is time to update the MSK, the BM-SC sends MIKEY message over UDP transporting the requested MSKs to the UE.

If requested by the BM-SC, the UE sends a MIKEY acknowledgement message to the BM-SC.

6.3.2.3.2 ~~Push solicited pull~~Void

~~While the push is the regular way of updating the MSK to the UE, there may be situations where the BM-SC solicits the UE to contact the BM-SC and request for new MSKs. An example of such situation is when the BM-SC wants the UE to authenticate itself during the service or when the MUK has expired.~~



~~**Figure 6.3: Push solicited pull**~~

~~The BM-SC sends MIKEY message over UDP to the UE. The key IDs in the extension payload of the MIKEY message set to 0x0 to indicate that the UE should request for current MSK from the BM-SC.~~

~~When the UE contacts the BM-SC, the BM-SC may trigger re-authentication of the UE or even re-run of GBA procedure to update the MUK.~~

~~The rest of the procedure is the same as in 6.3.1.~~