Source: **SA WG3**

Title: **19 CRs to 33.246: (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CRs have been agreed by SA WG3 and are presented to TSG SA for approval.

TSG SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Work item
SP-040859	33.246	001	4	Rel-6	Deletion of MBMS keys stored in the ME	C	6.0.0	S3-041122	MBMS
SP-040859	33.246	002	-	Rel-6	Clarification on key management	C	6.0.0	S3-040744	MBMS
SP-040859	33.246	005	3	Rel-6	Clean up of MBMS TS	D	6.0.0	S3-041115	MBMS
SP-040859	33.246	006	1	Rel-6	Traffic protection combinations	F	6.0.0	S3-040852	MBMS
SP-040859	33.246	007	3	Rel-6	Clarifying ME and BM-SC capabilities	F	6.0.0	S3-041010	MBMS
SP-040859	33.246	009	1	Rel-6	MBMS MTK Download transport	C	6.0.0	S3-040853	MBMS
SP-040859	33.246	010	3	Rel-6	MBMS Transport of salt	C	6.0.0	S3-041125	MBMS
SP-040859	33.246	011	1	Rel-6	SRTP index synchronisation within ME	C	6.0.0	S3-040854	MBMS
SP-040859	33.246	012	2	Rel-6	Clarify the use of mandatory MIKEY features for MBMS	F	6.0.0	S3-041055	MBMS
SP-040859	33.246	014	-	Rel-6	Protection of the Gmb reference point	C	6.0.0	S3-040801	MBMS
SP-040859	33.246	015	1	Rel-6	Use of parallel MSKs and MTKs	C	6.0.0	S3-040859	MBMS
SP-040859	33.246	016	3	Rel-6	Scope of MBMS security	C	6.0.0	S3-041116	MBMS
SP-040859	33.246	018	4	Rel-6	Clarification of the format of MTK ID and MSK ID	C	6.0.0	S3-041120	MBMS
SP-040859	33.246	020	3	Rel-6	MTK update procedure for streaming services	B	6.0.0	S3-041117	MBMS
SP-040859	33.246	021	8	Rel-6	Clarification of MSK key management	C	6.0.0	S3-041126	MBMS
SP-040859	33.246	022	1	Rel-6	Modification of delivery of MIKEY RAND field in MSK updates	C	6.0.0	S3-040856	MBMS
SP-040859	33.246	023	2	Rel-6	OMA DRM DCF for protection of download services	C	6.0.0	S3-041128	MBMS
SP-040859	33.246	028	1	Rel-6	Shorter MKI	C	6.0.0	S3-041119	MBMS
SP-040859	33.246	033	1	Rel-6	Handling of MBMS identities and definition completion/modification Specify how to identify the MUK and MRK	C	6.0.0	S3-041127	MBMS

3GPP TSG-SA3 Meeting #36
Shenzhen, China, 23-26 October 2004

Tdoc ⌘ S3-041122

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **001** ⌘ **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 ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Deletion of MBMS keys stored in the ME
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	23/11/2004
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:

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 ME behaviour at UICC change and ME power down for ME based key management is unspecified. This behaviour needs to be specified as it is relevant for security and key request overhead. If the ME deletes the MSK at power down, then the MBMS user will need to request MSK to the BM-SC (http request) and may need to run GBA to reconvene an MBMS session after power on. From a security point of view the deletion of these ME stored MBMS keys at power down is not necessary provided that the same UICC is used at power up. Consequently only at detecting a UICC change all MBMS keys shall be deleted.
Summary of change:	⌘	For ME based key management a) All MBMS keys (MUK, MRK, MSK and MTK) shall be deleted from the ME when a different UICC is inserted. b) All MBMS keys (MRK, MSK and MTK) may be deleted from the ME when the ME is powered down. If the ME does not delete the MBMS keys then the MBMS keys need to be stored in non-volatile memory. c) The ME should store the MUKs in non-volatile memory in order to be able to authenticate the first MIKEY message of a push solicited pull procedure
Consequences if not approved:	⌘	

Clauses affected:	⌘	6.1

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

Other comments:	⌘	

***** Begin of change *****

6 Security mechanisms

6.1 Using GBA for MBMS

GBA[6] 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.

An 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 [6] clause 5. The BM-SC will act as a NAF according to [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 to protect MSK deliveries to the UICC as described within subclause 6.3. The key Ks_ext_NAF is used as the key MRK within the protocols as described within subclause 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 subclause 6.3. The key MRK is used to authenticate the UE towards the BM-SC within the protocols as described within subclause 6.2.

For ME based key management

- All MBMS keys (MUK, MRK, MSK and MTK) shall be deleted from the ME when a different UICC is inserted. Therefore the ME needs to store in non-volatile memory the last inserted UICC-identity to be able to compare that with the used UICC-identity at UICC insertion and power on.
- All MBMS keys (MRK, MSK and MTK) may be deleted from the ME when the ME is powered down. If the ME does not delete the MBMS keys at power down then the MBMS keys need to be stored in non-volatile memory. The ME should store the MUKs in non-volatile memory in order to be able to authenticate the first MIKEY message of a push solicited pull procedure (cf. clause 6.3.2.2.4).

NOTE: If the ME deletes the MSK at power down, then the MBMS client would need to request MSK to the BM-SC and may need to run GBA to reconvene an MBMS session.

***** End of change *****

3GPP TSG-SA WG3 Security Meeting #35
St Paulís Bay, Malta, 5-8 October 2004

Tdoc ⌘S3-040744

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **002** ⌘ **rev** **-** ⌘ 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 on key management
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	24/09/2004
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:

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:	⌘	Alignment with TS 22.146. CR to TS 22.146 SP 040696 which was approved at SA#25 states : " If a terminal supports MBMS, then it shall support UICC based key management and all the function and interfaces required for it. In addition, ME key management shall be supported. If the UICC is capable of MBMS key management, ME key management shall not be activated."
Summary of change:	⌘	Clarify that UICC based key management is used when UICC is capable of MBMS key management and that ME based key management is used when UICC is not capable of MBMS key management.
Consequences if not approved:	⌘	Misalignment between TS 22.146 and TS 33.246

Clauses affected:	⌘	3.1, 6.1

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

Other comments:	⌘	

***** Begin of 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 [5].

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 MSKís to the UE.

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

***** End of change *****

***** Begin of change *****

6 Security mechanisms

6.1 Using GBA for MBMS

GBA[6] 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.

An 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 [6] clause 5. The BM-SC will act as a NAF according to [6].

The MSKs for an MBMS User service shall be stored on either the UICC if the UICC is capable of MBMS key management or the ME if the UICC is not capable of MBMS key management.

~~-~~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 to protect MSK deliveries to the UICC as described within subclause 6.3. The key Ks_ext_NAF is used as the key MRK within the protocols as described within subclause 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 subclause 6.3. The key MRK is used to authenticate the UE towards the BM-SC within the protocols as described within subclause 6.2.

***** End of change *****

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

Tdoc ⌘S3-041115

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **005** ⌘**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⌘ ☐ ME [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	Clean up of MBMS TS
Source:	⌘	SA WG3
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 ñ 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 ì double cipheringî 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 Security ó S3#35
St Paul's Bay, Malta, 5ñ8 October 2004

Tdoc ⌘ S3-040852

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **006** ⌘ **rev** **1** ⌘ 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:	⌘	Traffic protection combinations
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	27/09/2004
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:	⌘	To clarify the allowed combinations of confidentiality and integrity protection
Summary of change:	⌘	The current text in 5.3 specifying the combinations of confidentiality and integrity protection for MBMS are unclear and are also contradictory with the requirements in annex C. The allowed combinations in the protection of the traffic for MBMS service are clarified: - no protection - confidentiality protection and integrity protection - confidentiality protection only - integrity protection only
Consequences if not approved:	⌘	The allowed combinations of confidentiality and integrity protections remains unclear.

Clauses affected:	⌘	5.3

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

⌘

Other comments: ⌘

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 requires no additional protection). If t~~T~~his protection is required, it will be either confidentiality and integrity or ~~just~~ confidentiality only or integrity only. 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.

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

Tdoc ⌘S3-041010

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **007** ⌘ **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⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Clarifying ME and BM-SC capabilities
Source:	⌘	SA WG3
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 4.2 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. - Some editorial enhancements to section 6.1 including deletion of superfluous text.
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 ñ 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 a~~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~~A run of GBA_ME 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 #35
Malta, 5 ñ 8 October

Tdoc ⌘S3-040853

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **009** ⌘ **rev** **1** ⌘ 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 MTK Download transport
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	22/09/2004
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 delivery of MTK must be specified.
Summary of change:	⌘	A section stating how the MIKEY message containing the MTK is delivered over the same FLUTE stream as the actual downloaded object. The details on how the messages are carried in FLUTE should be specified by SA4.
Consequences if not approved:	⌘	There will not be a way to get the MTK from the BM-SC to the UE in the download case.

Clauses affected:	⌘	2, 6.3.3.2

		Y	N			
Other specs Affected:	⌘	X		Other core specifications	⌘	26.346
			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] 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: "Multimedia Broadcast/Multicast Service; Protocols and Codecs".

__SECOND_CHANGE__

6.3.3.2 MTK update procedure

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

6.3.3.2.1 MTK delivery in download

In the download case the MIKEY message carrying the MTK shall be delivered over the same FLUTE stream as the object to be downloaded to the UE [13]. This means that the message is specified as a separate object in the FLUTE File Delivery Table (FDT), having its own identifier. The mime-type of the object carrying the MIKEY message shall be the IANA-registered type for MIKEY.

3GPP TSG-SA3 Meeting #36 ***Tdoc ⌘S3-04111825***
Shenzhen, China, 23 ñ 26 November 2004

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **010** ⌘**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:	⌘	MBMS Transport of salt
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	23/11/2004
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 protection of the MBMS traffic will not meet the commonly required design goal of having a security level equivalent to the key size.
Summary of change:	⌘	The salt needed by SRTP is sent in the KEMAC payload of the MIKEY message containing the MTK.
Consequences if not approved:	⌘	The protection of the MBMS traffic may be vulnerable to pre-computation attacks.

Clauses affected:	⌘	6.4.5.3, 6.4.6.2, 6.5.4, D.3

		Y	N			
Other specs Affected:	⌘	X		Other core specifications	⌘	TS 31.102
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

__FIRST_CHANGE__

6.4.5.3 MTK message structure

The structure of the MIKEY message carrying a MTK key is depicted in Figure 6.7. The actual key that is delivered is kept in the KEMAC payload. If MTK is to be used for streaming protection, then a 112 bit salt shall be added to the KEMAC payload in addition to the MTK. The network identity payloads (IDi) shall be used in MTK transport messages.

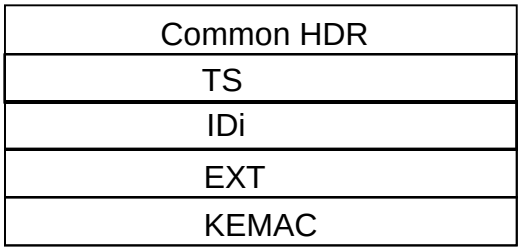


Figure 6.7: The logical structure of the MIKEY message used to deliver MTK

__SECOND_CHANGE__

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 [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 is larger or equal to the current MIKEY replay counter associated with the given MSK (the 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 and salt if available) or failure.

__THIRD_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 [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.

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

In the case of streaming, SRTP requires a master key and a master salt. The MTK is used as master key, and the salt in the KEMAC payload is used as master salt.

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 MIKEY [9].

__FOURTH_CHANGE__

D.3 MTK generation and validation

This procedure is part of the MTK generation and validation function as described in clause 6.5.4 (MTK validation and derivation).

The ME receives the MIKEY message (containing Header, Time stamp, Network ID, Key Group ID, MSK ID, MTK ID = SEQp, MSK_C[MTK||Salt (if salt is available)] and MAC). After performing some validity checks, the ME sends the whole message to the UICC. The UICC computes the MGV-F function as described in clause 6.5. (Validation and key derivation functions in MGV-F). After successful MGV-F procedure the UICC returns the MTK.

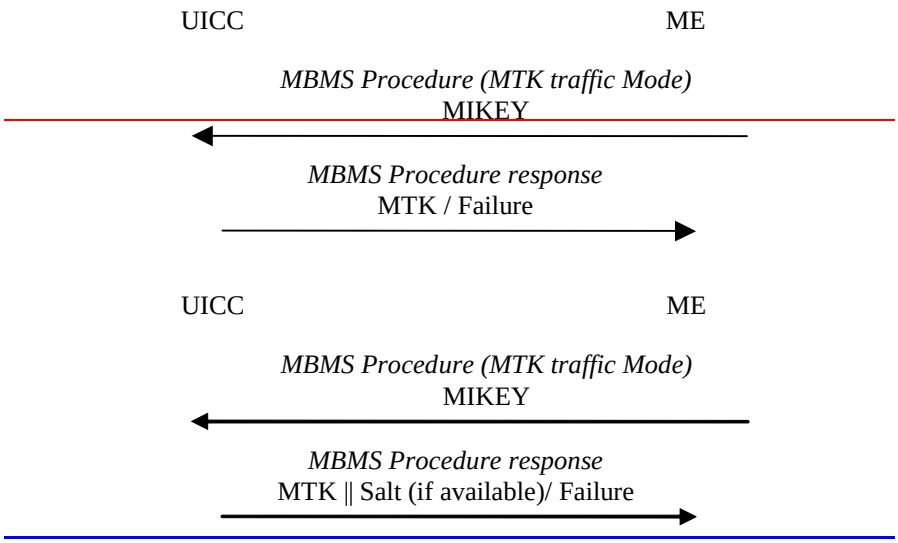


Figure D.3: MTK Generation and Validation

3GPP TSG-SA WG3 Meeting S3#35
St Paul's Bay, Malta, October 5-8, 2004

Tdoc ⌘S3-040854

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **011** ⌘ **rev** **1** ⌘ 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:	⌘	SRTP index synchronisation within ME
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	28/09/2004
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:

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:	⌘	Once the MBMS receiver has lost SRTP index synchronisation on a stream then he will be unable to further decrypt and authenticate the SRTP packets of the same SRTP session.
Summary of change:	⌘	Add the missing functionality: - Specify how to synchronise the SRTP Roll-over-counter
Consequences if not approved:	⌘	It will remain unspecified yet how an MBMS receiver can synchronise the SRTP Roll-over counter, and hence this might lead to the inability of MBMS streaming receivers to reconvene the MBMS session after being out of radio coverage for some time.

Clauses affected:	⌘	6.6.2

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

Other comments:	⌘	

===== BEGIN 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 [11] shall be used. The MTK is carried to the UEs from the BM-SC using MIKEY [9] 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 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 [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 [9].

SRTP security policy parameters, such as encryption algorithm, are transported in MIKEY Security Policy payload as defined in chapter 6.10.1 in [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 subclause 6.3.

If the SRTP module has lost synchronisation on the ROC (Roll-over counter) of the SRTP stream, it shall wait for the next MTK update message received within the ptm stream. The BM-SC shall deliver the current ROC-value within the CS ID map info payload of the MIKEY common header payload.

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

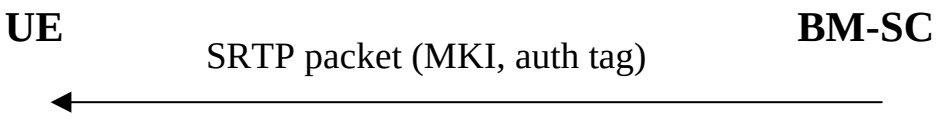


Figure 6.8: Delivery of protected streaming content to the UE

3GPP TSG-SA3 Meeting #36
Shenzhen, China, 23-26 October 2004

Tdoc S3-041055

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**012**	⌘	**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:	⌘	Clarify the use of mandatory MIKEY features for MBMS
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	16/11/2004
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:	⌘	MIKEY (IETF: "MIKEY: Multimedia Internet KEYing", http://www.ietf.org/internet-drafts/draft-ietf-msec-mikey-08.txt, Work In Progress.) specifies 1) in clause 3.2 that the public key encryption method is mandatory to implement. 2) in clause 6.6 that Timestamps payload types NTP-UTC and NTP are mandatory to implement The above functionality is not needed for MBMS key management, so there can be doubt if the MBMS implementation is standard compliant if it has not realized the above functions when reading the MIKEY RFC. Explicitly mentioning the not needed mandatory functions in the MBMS TS - require less effort then listing all required functions and payloads - allow faster time to market as there will be no doubt about the (not) required MIKEY features
Summary of change:	⌘	Specify in a new Annex the not required mandatory MIKEY functionality
Consequences if not approved:	⌘	It will remain unclear if the MBMS UE and BM-SC shall implement certain MIKEY features.

Clauses affected:	⌘	New Annex			
Other specs affected:	⌘	**Y**	**N**		
			N	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

Annex E (Informative): MIKEY features not used in MBMS

- An MBMS capable ME/UICC and BM-SC do not need to implement the public key encryption method of MIKEY (clause 3.2 of [9]) and related payloads, although mentioned in [9] as mandatory for implementation.
- An MBMS capable ME/UICC and BM-SC do not need to implement the Time Stamp payload types NTP-UTC and NTP of MIKEY (clause 6.6 of [9]) although mentioned in [9] as mandatory for implementation.

3GPP TSG-SA WG3 Meeting S3#35
St Paul's Bay, Malta, October 5-8, 2004

Tdoc ⌘S3-040801

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **014** ⌘ **rev** **-** ⌘ 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 **X**

Title:	⌘	Protection of the Gmb reference point
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	27/09/2004
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:
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 DIAMETER protocol has been specified within TS 29.061 for use on the Gmb reference point. Since DIAMETER runs over IP and since the Gmb reference point (GGSN - BM-SC or GGSN - Gmb proxy - BM-SC) always resides within an operatorís network, NDS/IP protection may be used (TS 33.210) according to Za or Zb reference points.
Summary of change:	⌘	Removal of the Editorís Note that the Gmb reference point security is for ffs. Add NOTE that NDS/IP mechanism may be used for securing the Gmb reference point.
Consequences if not approved:	⌘	Gmb reference point protection remains unspecified

Clauses affected:	⌘	2, Annex C
Other specs affected:	⌘	Y N ☐ **N** Other core specifications ☐ **N** Test specifications ☐ **N** O&M Specifications
Other comments:	⌘	

===== BEGIN 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] 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 33.210: "Network domain security; IP network layer security".

===== END CHANGE =====

===== BEGIN NEXT CHANGE =====

Annex C (normative): Multicast security requirements

C.1 Requirements on security service access

C.1.1 Requirements on secure service access

R1a: A valid USIM shall be required to access MBMS User Services.

R1b: It shall be possible to prevent intruders from obtaining unauthorized access of MBMS User Services by masquerading as authorized users.

C.1.2 Requirements on secure service provision

R2a: It shall be possible for the network (e.g. BM-SC) to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorized access to MBMS User Services.

R2b: It shall be possible to prevent the use of a particular USIM to access MBMS User Services.

NOTE: No security requirements shall be placed on the UE that requires UE to be customised to a particular customer prior to the point of sale.

C.2 Requirements on MBMS transport Service signaling protection

R3a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS transport service signaling on the Gmb reference point.

NOTE: This requirement may be fulfilled by physical or proprietary security measures if the Gmb protocol endpoints (i.e. GGSN, Gmb-Proxy and BM-SC) are located within the same security domain of the operatorís network. Otherwise the security mechanisms as specified within 33.210 [13] shall be applied.

~~Editor's Note: When the Gmb reference point is IP-based then NDS/IP methods according to TS 33.210 may be applied to fulfill requirement R3a. The Gmb interface is ffs.~~

R3b: Unauthorized modification, insertion, replay or deletion of all transport service signaling, on the RAN shall be prevented when the RAN selects a point-to-multipoint (ptm) link for the distribution of MBMS data to the UE.

NOTE: UTRAN Bearer signalling integrity protection will not be provided for point to multipoint MBMS signalling and GERAN has no bearer signalling integrity protection, even for point to point signalling.

C.3 Requirements on Privacy

R4a: The User identity should not be exposed to the content provider or linked to the content in the case the Content Provider is located outside the 3GPP operator's network.

R4b: MBMS identity and control information shall not be exposed when the RAN selects a point-to-multipoint link for the distribution of MBMS data to the UE.

NOTE: UTRAN and GERAN Bearer confidentiality protection will be not be provided for point to multipoint MBMS sessions.

C.4 Requirements on MBMS Key Management

R5a: The transfer of the MBMS keys between the MBMS key generator and the UE shall be confidentiality protected.

R5b: The transfer of the MBMS keys between the MBMS key generator and the UE shall be integrity protected.

R5c: The UE and MBMS key generator shall support the operator to perform re-keying as frequently as it believes necessary to ensure that:

- users that have joined an MBMS User Service multicast service, but then left, shall not gain further access to the MBMS User Service without being charged appropriately
- users joining an MBMS User Service shall not gain access to data from previous transmissions in the MBMS User Service without having been charged appropriately
- the effect of subscribed users distributing decryption keys to non-subscribed users shall be controllable.

R5d: Only authorized users that have joined an MBMS User Service shall be able to receive MBMS keys delivered from the MBMS key generator.

R5e: The MBMS keys shall not allow the BM-SC to infer any information about used UE-keys at radio level (i.e. if they would be derived from it).

R5f: All keys used for the MBMS User Service shall be uniquely identifiable. The identity may be used by the UE to retrieve the actual key (based on identity match, and mismatch recognition) when an update was missed or was erroneous/incomplete.

R5g: The BM-SC shall be aware of where all MBMS specific keys are stored in the UE (i.e. ME or UICC).

R5h: The function of providing MTK to the ME shall only deliver a MTK to the ME if the input values used for obtaining the MTK were fresh (have not been replayed) and came from a trusted source.

C.5 Requirements on integrity protection of MBMS User Service data

R6a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS User Service data sent to the UE on the radio interface. The use of integrity shall be optional.

NOTE: It may be possible to detect the deletion of MBMS data packets, but it is impossible to prevent the deletion. Packets may be lost because of bad radio conditions, providing integrity protection will not help to detect or recover from this situation.

NOTE: The use of shared keys (integrity and confidentiality) to a group of untrusted users only prevents attacks of lower levels of sophistication, such as preventing eavesdroppers from simply listening in

R6b: The MBMS User Service data may be integrity protected with a common integrity key, which shall be available to all users that have joined the MBMS User Service.

R6c: It may be required to integrity protect the "BM-SC - GGSN" interface i.e. reference point Gi.

C.6 Requirements on confidentiality protection of MBMS User Service data

R7a: It shall be possible to protect the confidentiality of MBMS User Service data on the radio interface.

R7b: The MBMS User Service data may be encrypted with common encryption keys, which shall be available to all users that have joined the MBMS User Service.

R7c: It may be required to encrypt the MBMS User Service data on the "BM-SC - GGSN" interface, i.e. the reference points Gi.

R7d: It shall be infeasible for a man-in-the-middle to bid down the confidentiality protection used on protect the MBMS User Service from the BM-SC to the UE.

R7e: It shall be infeasible for an eavesdropper to break the confidentiality protection of the MBMS User Service when it is applied.

C.7 Requirements on content provider to BM-SC reference point

R8a: The BM-SC shall be able to authenticate and authorize a 3rd party content provider that wishes to transmit data to the BM-SC.

R8b: It shall be possible to integrity and confidentiality protect data sent from a 3rd party content provider to the BM-SC.

NOTE: This reference point will not be standardised.

===== END CHANGE =====

3GPP TSG-SA3 Meeting #35
St Paulís Bay, Malta, October 5 ñ 8, 2004

Tdoc ⌘S3-040859

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **015** ⌘ **rev** **1** ⌘ 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:	⌘	Use of parallel MSKs and MTKs
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	28/09/2004
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 use of parallel MSKs and MTKs is unclear.
Summary of change:	⌘	The use of parallel MSKs and MTKs is clarified: There shall be only one MSK and MTK in use within one Key Group ID. I.e. parallel use of two or more MSKs (with different MSK IDs) or MTKs (with different MTK IDs) within a Key Group ID shall not be allowed.This is due to the fact that MSK ID and MTK ID are sequence numbers. I.e. the UE would discard the MSK/MTK with smaller MSK ID/MTK ID. The use of the same MTK with two different transport services (or user services) should be avoided. This is to avoid synchronization problems in the UE when a new MTK is taken into use in the traffic. I.e. if the MTK is not changed synchronously in the traffic flows the UE would discard the traffic with smaller MTK ID.
Consequences if not approved:	⌘	Use of MSKs and MTKs remains underspecified.

Clauses affected:	⌘	4.2

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

Other comments: ⌘

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 MBMS Service Keys (MSKs) to secure the different Transport Services that make up the MBMS User Service. The MSKs are not directly used to secure the MBMS Transport Services, but they are used to protect the delivery of MBMS Transport Keys (MTKs), which are used to secure the MBMS Transport Services, as specified within subclauses 6.5 and 6.6. MSKs and MTKs are managed at the MBMS User Service Level.

There shall be only one MSK and MTK in use within one Key Group ID. I.e. parallel use of two or more MSKs (with different MSK IDs) or MTKs (with different MTK IDs) within a Key Group ID shall not be allowed.

~~NOTE: According to good security practice the~~ The use of the same MTK (this implies also the same MSK) with two different ~~security protocols~~ transport services (or user services) ~~shall~~ should be avoided.

NOTE: This is to avoid synchronization problems in the UE when a new MTK is taken into use in the traffic. I.e. if the MTK is not changed synchronously in the traffic flows the UE would discard the traffic with smaller MTK ID.

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

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

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: ⌘

******* 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] 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: ì Multimedia Broadcast/Multicast Service, Protocols and codecsî

******* 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: ì Multimedia Broadcast/Multicast Service, Protocols and codecsî [13].

MBMS streaming session: See TS 26.346: ì Multimedia Broadcast/Multicast Service, Protocols and codecsî [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 MSKís 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 ⌘S3-041120

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **018** ⌘ **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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Clarification of the format of MTK ID and MSK ID.
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 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 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:	⌘				

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

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 every time the MTK is updated. The MTK ID shall be reset every time the MSK is updated.

~~Editorís 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~~ 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.

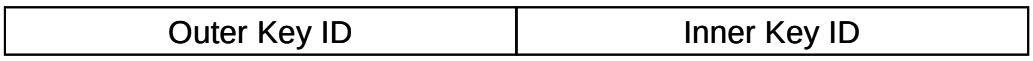


Figure 6.4: Extension payload used with MIKEY

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 ⌘S3-041117

CR-Form-v7.1

CHANGE REQUEST

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

Title:	⌘	MTK update procedure for streaming services
Source:	⌘	SA WG3
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: ⌘

****** FIRST 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.

Editorís 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.

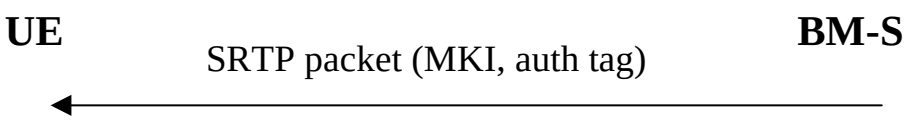


Figure 6.8: Delivery of protected streaming content to the UE

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

Tdoc ⌘S3-041126

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **021** ⌘ **rev** **8** ⌘ 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:	⌘	Clarification of MSK key management
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	25/11/2004
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. Required Security parameters in Service Annoucement are 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.
Summary of change:	⌘	Initiation of key management is specified. Required Security parameters in Service Annoucement are specified. The details of UE requesting for MSKs is specified. The details of BM-SC solicited pull are specified. The BM-SC shall be allowed to use a MUK beyond the ks_xx_NAF lifetime for the purpose of MSK update trigger.
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)

Other specs affected:	⌘	Y	N		⌘
			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] 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 *******

6.3.2.2 ~~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 MSK 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;

~~Editorís 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~~

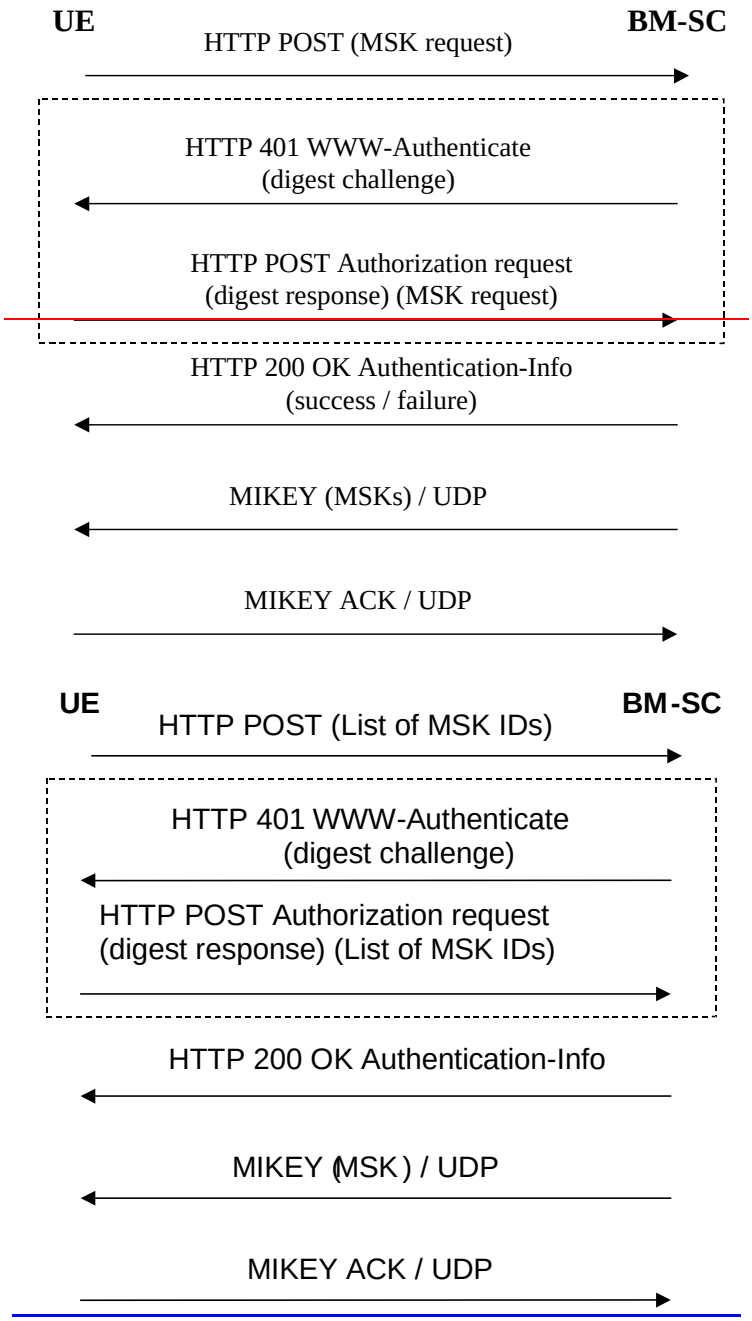


Figure 6.x~~1~~: ~~UE initiated MSK delivery~~Basic MSK retrieval procedure

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 MSK IDs~~.~~

NOTE: When the Key Number part of the MSK ID is set to 0x0, this means the current MSK, see clause 6.3.2.1.

Editorsí 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.~~

If the authentication is successful then t~~T~~he 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.~~If the authentication fails then the BM-SC resends HTTP 401 Authorization required message with the WWW-Authenticate header.

Editorsí 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:

- Fully qualified 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
- UICC key management required: yes/ no
- Identifiers of the MSKs needed for the User Service

  The Key Number part of the MSK ID(s) shall be set to 0x0 to denote the current MSK. Specific Key Number values are not used since they may change over time and Key Group part of MSK ID is sufficient to identify the MSKs, see clause 6.3.2.1.
- Mapping information how the MSKs are used to protect the different User Service Sessions

Editorsí 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.

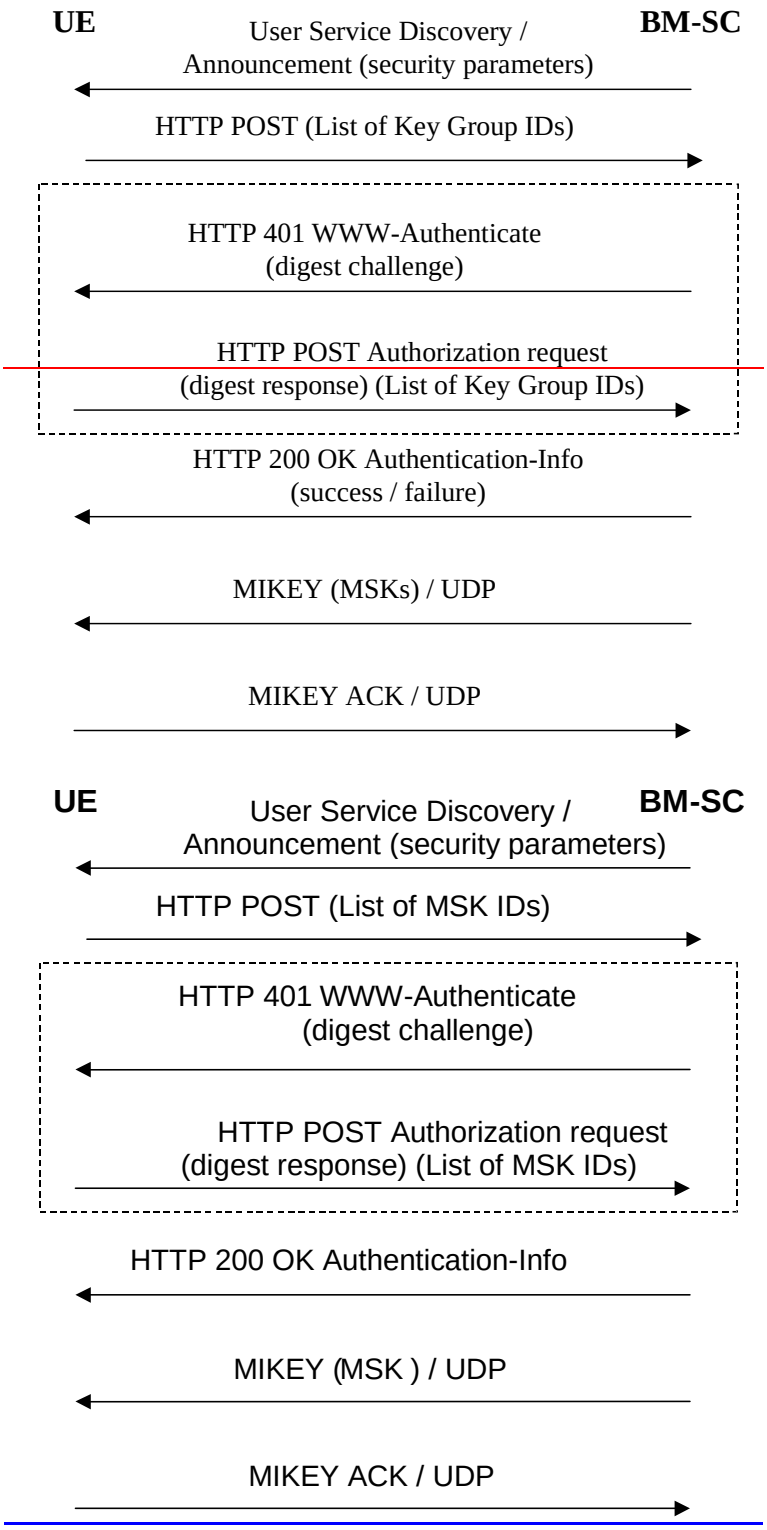


Figure 6.x: MSK retrieval procedure

In case the UICC key management is required, the UE should only try to access the MBMS user service if the used UICC application is capable of MBMS key management.

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.

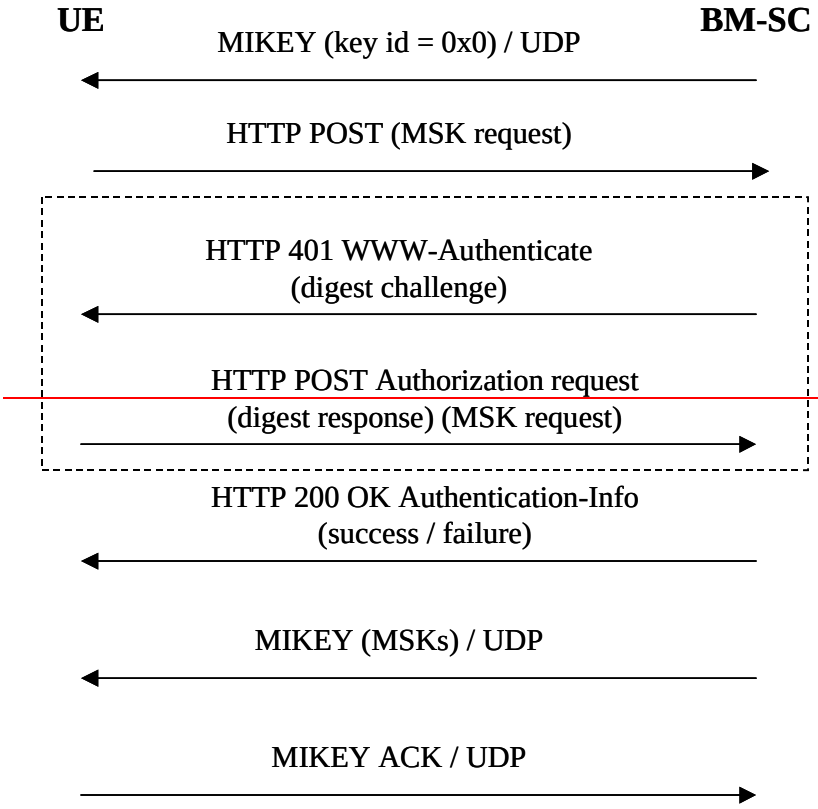
The rest of the procedure is the same as in 6.3.2.3.1.

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. An example of such a situation is when the BM-SC wants the UE to trigger a UE that it needs to update the MSK.



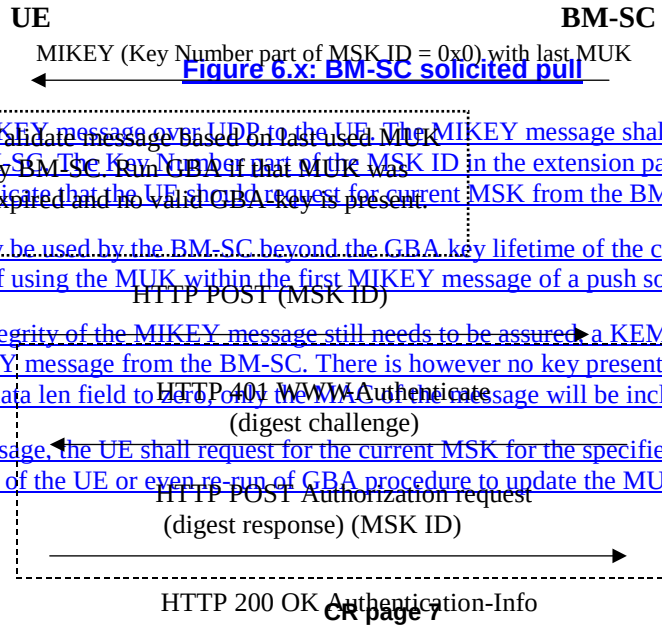


Figure 6.x: BM-SC solicited pull

The BM-SC sends a MIKEY message over UDP to the UE. The MIKEY message shall be protected by the most recent MUK known by the BM-SC. The Key Number part of 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: A MUK may be used by the BM-SC beyond the GBA key lifetime of the corresponding Ks_xx_NAF for the purpose of using the MUK within the first MIKEY message of a push solicited pull procedure.

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 current 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.

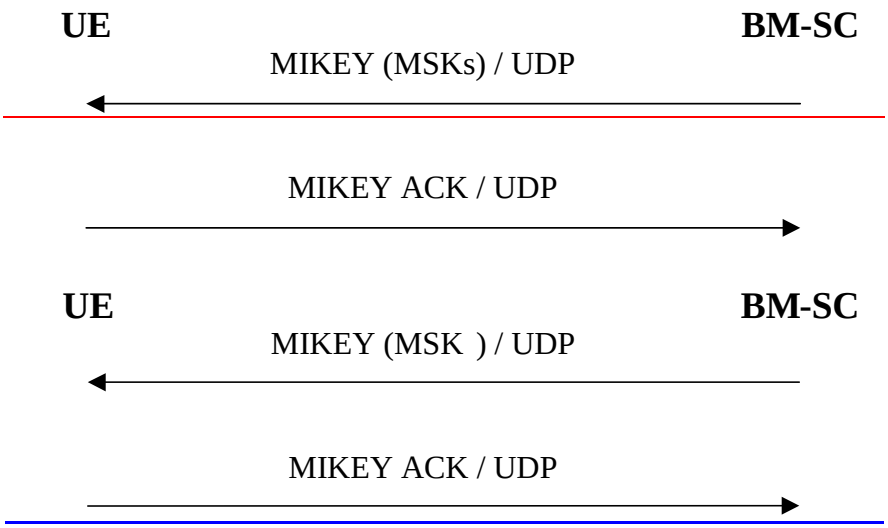


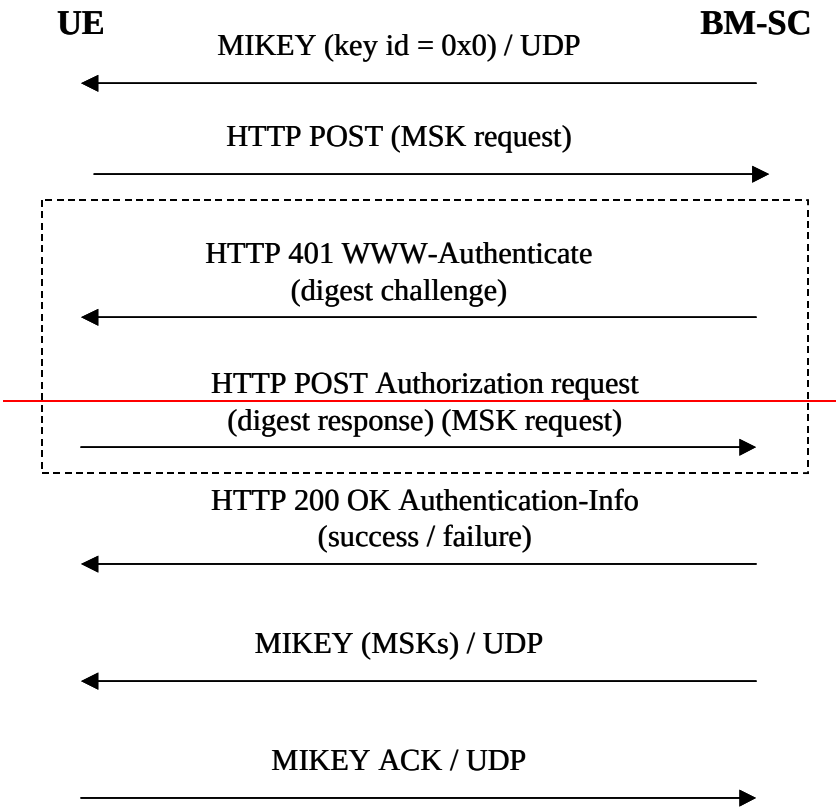
Figure 6.2: Pushing the MSKs to the UE

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.~~

3GPP TSG SA WG3 Meeting S3#35
St Paul's Bay, Malta, 5 ñ 8 October 2004

Tdoc ⌘S3-040856

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **022** ⌘ **rev** **1** ⌘ 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 [ ]

Title:	⌘	Modification of delivery of MIKEY RAND field in MSK updates
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	20/09/2004
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:

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:	⌘	Currently, TS states that MIKEY-RAND is only delivered in the first MIKEY packet containing an MSK update message. Basically, that imposes to the MGV-F the need to store MIKEY-RAND together with a given MUK for further MUK & MSK derivation. That also implies that when receiving MSKs from different BMSCs (e.g. roaming situations) the storage of multiple MUK and associated MIKEY_RAND parameter (one per BMSC) is required. Contrary to MUK, which can be derived in the UE from existing GBA keys, there is no way to retrieve MIKEY_RAND value if for any reasons it is missed or replaced. If that happens, the BM-SC cannot be aware that MIKEY RAND is no more present in the UE. So, if the same MUK is used again to deliver a MSK, BM-SC will not include MIKEY-RAND in his MSK update message. As a consequence MUK & MSK derivation procedures cannot take place and the MSK update procedure will fail.
Summary of change:	⌘	MIKEY RAND is sent in all MSK update MIKEY packets. MIKEY RAND will be used for MUK derivation whenever MUK_C and MUK_I are not present. MIKEY RAND will always be used for MSK derivation (MSK_I and MSK_C) whenever a new MSK is sent. Then, the MGV-F does not need to store MIKEY_RAND fields.
Consequences if not approved:	⌘	Unnecessary complexity in handling replacement of MUK and associated parameters. Possible scenarios where MSK update procedure are not possible unless a complete GBA bootstrap procedure is performed.

Clauses affected:	⌘	
Other specs affected:	⌘	Y / N [ ] / [X] Other core specifications ⌘ [ ] / [X] Test specifications [ ] / [X] O&M Specifications
Other comments:	⌘	6.4.5.1

6.4.5 MIKEY message structure

6.4.5.1 MSK message structure

The structure of the MIKEY message carrying a MSK key is depicted in Figure 6.5. The actual key that is delivered is kept in the KEMAC payload. The MIKEY-RAND is used to derive e.g. encryption and authentication keys from the received keys. It is sent ~~only~~ in all the ~~initial~~ MSK delivery messages. The identity payloads of the initiatorís and responderís IDs shall be included in the MSK transport messages. IDi is the ID of the BM-SC and IDr is the ID of the UE. Security Policy (SP) payload includes information for the security protocol such as algorithms to use, key lengths, initial values for algorithms etc. The Key Validity Data subfield is present in the KEMAC payload when MSK is transported but it is not present for MTK transport. The field defines the Key Validity Time for MSK in terms of sequence number interval (i.e. lower limit of MTK ID and upper limit of MTK ID). The lower limit of the interval defines the SEQs to be used by the MGV-F (see subclause 6.5).

Editorís Note: The type (URI or NAI) of identity payloads to use are for further study.

Editorís Note: The contents of the Security Policy payload depends on the used security protocols. MIKEY [9] has defined Security Policy payload for SRTP, but for other security protocols there is a need to define new Security Policy payloads. The exact definitions of these are FFS.

3GPP TSG SA WG3 Security ó S3#36
Shenzhen, China, 23ñ26 November 2004

Tdoc ⌘ S3-041128

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **023** ⌘ **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:	⌘	OMA DRM DCF for protection of download services
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	28/10/2004
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:

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 to protect the MBMS download services
Summary of change:	⌘	Describes how OMS DRM DCF is used for download protection
Consequences if not approved:	⌘	It will remain unspecified how to protect the MBMS download services.

Clauses affected:	⌘	2, 6.5.4, 6.6.3			
Other specs affected:	⌘	**Y** Other core specifications	⌘	26.346	
		N Test specifications			
		N 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] 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] ì OMA DRM Content Formatî , OMA-DRM-DCF-v2_0, www.openmobilealliance.org.

****** 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.

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).

In case of download service, MIKEY key derivation as defined in Section 4.1.3 of MIKEY [9] shall be used to derive MTK authentication and encryption keys from MTK in the ME. These keys shall be provided to the download protection protocol.

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

6.6.3 Protection of download content

Editor's Note: The details of MBMS download protection are subject to the response from OMA BAC DLDRM. SA3 has asked OMA BAC DLDRM whether it is possible to include the extensions and deviations needed for using the DCF format for MBMS download protection to OMA DRM v2.0 DCF specification. If the answer is positive, some material in this section will be removed and the OMA specification referenced instead.

6.6.3.1 General

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.

6.6.3.2 Usage of OMA DRM DCF

When it is required to protect MBMS download content, OMA DRM V2.0 DCF as defined in [13] shall be used. MBMS download contents are indicated by the 3GPP-MBMS-DCF flag in the Common Headers Box of a DCF. OMA DRM Rights Objects are not utilized. Instead, encryption and authentication keys are generated from MTK. For integrity protection, an MBMSSignature as specified below is attached in the FreeSpaceBox of the DCF.

The MBMSSignature Box is an extension to OMA DRM V2.0 DCF for use by MBMS, and is defined as follows:

```
aligned(8) class MBMSSignature extends Fullbox('sign', version, flags) {
   Unsigned int(8)  SignatureMethod; // Signature Method
   Char    Signature[];   // Actual Signature
}
```

SignatureMethod Field:

NULL 0x00

HMAC-SHA1 0x01

The range of data for the HMAC calculation shall be according to Section 5.3 of [13].

The correct MTK for decrypting and verifying the integrity of the download content is indicated by the key_id in the RightsIssuerURL field as follows:

mbms-key://key_id

where key_id is defined as the base64 encoded concatenation (Key Domain ID || MSK_ID || MTK ID).

In case the FDT of the FLUTE protocol needs to be protected, the FDT may also be wrapped in a different DCF. Confidentiality and/or integrity protection of FDT can be provided this way.

Editors' note: The optionality of FDT protection is still under study (i.e. whether it should be mandated)

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

Tdoc ⌘S3-041119

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **028** ⌘ **rev** **1** ⌘ 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:	⌘	Shorter MKI
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	23/11/2004
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:	⌘	MKI field is too long, and contains unnecessary information. Also Section 6.6.2.2 is unclear in the sense that it gives the impression that the MKI needs to be globally unique. This is not the case; it only needs to be unique in any given SRTP context. The Network ID is known once the SRTP context is identified.
Summary of change:	⌘	Removed the Network ID from the MKI field.
Consequences if not approved:	⌘	The MKI will contain information that is not required for functionality and there will be a waste of bandwidth.

Clauses affected:	⌘	6.6.2.1, 6.6.2.2

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

Other comments:	⌘	

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 retrieve the correct cryptographic context identified by destination transport address, destination port and SSRC (according to RFC 3711), check if it has the MTK corresponding to the value in the MKI field in the SRTP cryptographic context.

NOTE: The cryptographic context needs to be unique for each SRTP stream.

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.

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

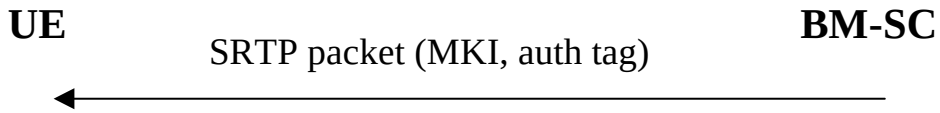


Figure 6.8: Delivery of protected streaming content to the UE

pop3GPP TSG-SA3 Meeting #36
Shenzen, China, 23 ñ 26 November

Tdoc ⌘ S3-041127

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **033** ⌘ **rev** **1** ⌘ 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:	⌘	Handling of MBMS identities and definition completion/modification
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	25/11/2004
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:	⌘	Specify the missing identification and how the identities are used and transported in the different field of the MIKEY delivery and response messages.
Summary of change:	⌘	MUK, MRK IDs are undefined and their use in MIKEY fields is unspecified. MTK, MSK, and Network ID are put into MIKEY extension field. MSK ID is redefined combining former MSK and Key Group IDs. Removed ID_i from the response message, since it is not needed and is not present in the MIKEY specification. The Network ID (MCC||MNC) is moved from the IDi field of MIKEY messages to the extension payload to obtain a uniform message structure for both MSK and MTK delivery. Network ID is renamed to Key Domain ID The Key IDs are carried as follows: For MSK delivery messages: MUK ID via IDi and IDr, MSK ID and Key Domain via extention payload. For MTK delivery messages: IDi and IDr and CSB are not used. MTK-ID, MSK-ID and Key Domain ID via extention payload. Adds dependency to IETF internet draft <draft-carrara-newtype-keyid-00.txt>
Consequences if not approved:	⌘	

Clauses affected:	⌘	2, 3.4 (New), 6.1, 6.3.2.1, 6.3.3.1, 6.4.1, 6.4.2, 6.4.4, 6.4.5, 6.4.6, 6.5.2, 6.5.3, 6.5.4, 6.6.2.1, Annex D

Other specs affected:	⌘	Y	N		⌘
		X		Other core specifications	TS 31.102
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

********** NEXT 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] 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] IETF internet draft "The Key ID Information Type for the General Extension Payload in MIKEYî <draft-carrara-newtype-keyid-00.txt>

** NEXT CHANGE ***

3.4 Conventions

All data variables in this specification are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bitstring. Where a variable is broken down into a number of substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

** NEXT CHANGE ***

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 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 to protect MSK deliveries to the UICC as described within clause 6.3. The key Ks_ext_NAF is used as the key MRK 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.

The MUK is identified by the combination of B-TID and NAF-ID and the MRK is defined by B-TID, where B-TID and NAF-ID are defined as specified in TS 33.220 [6].

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

6.3.2.1 MSK identification

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

where

~~Network~~ Key Domain 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 4~~2~~ bytes long and with byte 0 and 1 containing the Key Group part, and byte 2 and 3 containing the Key Number part. The Key Number part is used to distinguish MSKs that have the same ~~Network~~ Key Domain ID and Key Group ~~ID~~part. Key Group part is used to group keys together in order to allow redundant MSKs to be deleted. The MSK ID ~~It~~ is carried in the extension payload ~~MSK ID field~~ of MIKEY extension payload.

NOTE: It needs to be ensured that the Key Group parts are unique within an operator, i.e. two BM-SCs within an operator shall not use the same Key Group value.

If the UE receives an MSK and already contains two other MSKs under the same ~~Network~~ Key Domain ID and Key Group part~~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.

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

6.3.3.1 MTK identification

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

where

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

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

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

6.4 MIKEY message creation and processing in the ME

Editorís 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) [13] is added to MIKEY. The Extension Payload can contain the key types and identities of MSK and the MTK and Key Domain ID (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.~~is not used.

********** 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 key~~s~~ that is delivered in the message, a ~~new~~ general Extension Payload (EXT) with Type field value x is ~~defined~~ used that conforms to the structure defined in [13] ~~section 6.15 of RFC 3830 [9] (MIKEY)~~.

Editorís Note: The type value will be replaced by value requested from IANA.

The EXT includes a Key Domain ID and one or two Key Type ID sub-payloads depending on the message. These are used as follows.

For MSK delivery the EXT includes the Key Domain ID and a Key Type ID sub-payload. The Key Domain ID has the value as specified in clause 6.3.2.1. The Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MSK ID, see Figure 6.x. The key that is used to protect the message, i.e. MUK, is identified as specified in clause 6.1.

For MTK delivery the EXT includes the Key Domain ID and two Key Type ID sub-payloads. The Key Domain ID has the value as specified in clause 6.3.2.1. The first Key Type ID sub-payload includes the type and ID of the key that is used to protect the message, i.e. the MSK ID, and the second Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MTK ID, see Figure 6.y.

Editorís Note: The Key Domain ID needs to be added to [13]. It may need an extension payload type of its own.

~~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 different keys in use during the same session, where n is the number of bits in the ID field.

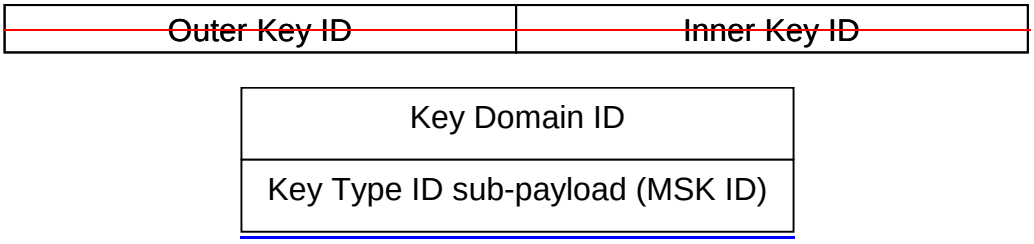


Figure 6.x4: Extension payload used with MIKEY MSK message

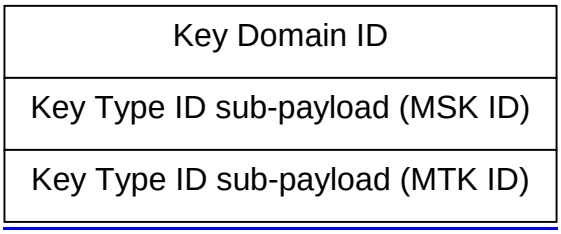


Figure 6.y: Extension payload used with MIKEY MTK message

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*********

6.4.5 MIKEY message structure

6.4.5.1 MSK message structure

The structure of the MIKEY message carrying a MSK key is depicted in Figure 6.5. The actual key that is delivered is kept in the KEMAC payload. The MIKEY-RAND is used to derive e.g. encryption and authentication keys from the received keys. It is sent only in the initial MSK delivery message. The identity payloads of the initiator's and responder's IDs shall be included in the MSK transport messages. IDi is the ID of the BM-SC (i.e. NAF-ID) and IDr is the ID of the UEís username (i.e.B-TID). Security Policy (SP) payload includes information for the security protocol such as algorithms to use, key lengths, initial values for algorithms etc. The Key Validity Data subfield is present in the KEMAC payload when MSK is transported but it is not present for MTK transport. The field defines the Key Validity Time for MSK in terms of sequence number interval (i.e. lower limit of MTK ID and upper limit of MTK ID). The lower limit of the interval defines the SEQs to be used by the MGV-F (see clause 6.5).

Editor's Note: The type (URI or NAI) of identity payloads to use are for further study.

Editor's Note: The contents of the Security Policy payload depends on the used security protocols. RFC 3830 [9] (MIKEY) has defined Security Policy payload for SRTP, but for other security protocols there is a need to define new Security Policy payloads. The exact definitions of these are FFS.

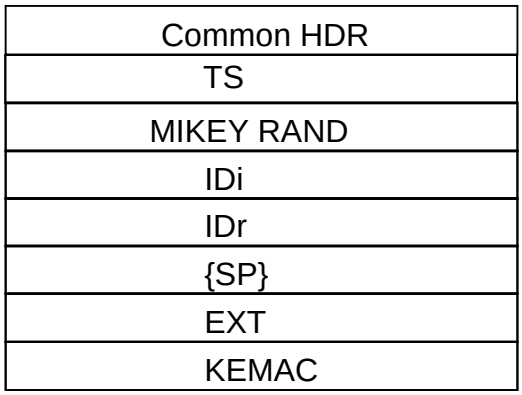


Figure 6.5: The logical structure of the MIKEY message used to deliver MSK. For use of brackets, cf. section 1.3 of RFC 3830 [9] (MIKEY)

6.4.5.2 MSK Verification message

If the BM-SC expects a response to the MSK-transport message (i.e., the V-bit in the MIKEY common header is equal to 1), the UE shall send a verification message as a response. The verification message shall be constructed according to section 3.1 of MIKEY, and shall consist of the following fields: HDR || TS ||~~ IDi_ ||~~ IDr || V, where ~~IDi is the ID of the BM-SC and~~ IDr is the ID of the UE. Note that the MAC included in the verification payload, shall be computed over both the initiator's and the responder's ID~~s~~ as well as the timestamp in addition to be computed over the response message as defined in RFC 3830 [9]. The key used in the MAC computation is the MUK_I.

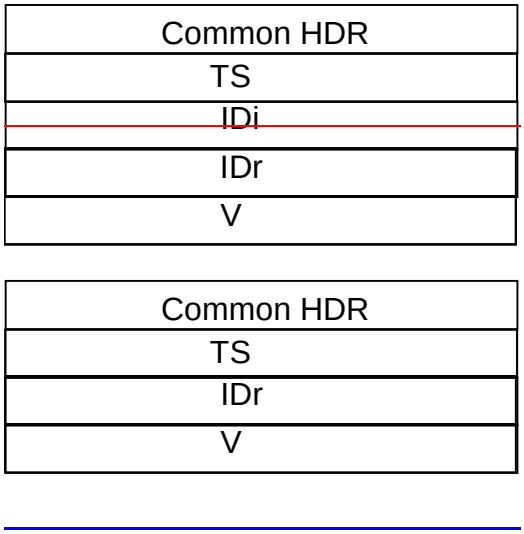


Figure 6.6: The logical structure of the MIKEY Verification message

The verification message shall not be sent as a response to MIKEY messages delivering MTK.

The verification message shall be constructed by the ME, except for the MAC field, and then be given to the MGV-F that will perform the MAC computation and will return the verification message appended with the MAC to the ME. The ME shall send the message to the BM-SC.

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

6.4.6 Processing of received messages in the ME

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 Extension Payload (~~Data Type field of the common MIKEY header (HDR)~~EXT) is examined, and if it indicates an MSK delivery protected with MUK, the MUK ID is received ~~extracted from the Extension Payload~~by combining IDi and IDr.
2. The Timestamp Payload is checked, and the message is discarded if the counter is larger or equal to the current MIKEY replay counter associated with the given MUK (the 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 RFC 1982 [10].
3. The Security Policy payload is stored if it was present.
4. The message is transported to MGV-F for further processing, cf clause 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 Extension Payload (~~Data Type field of the common MIKEY header (HDR)~~ EXT) is examined, and if it indicates an MT~~S~~K delivery protected with MSK, the MSK ID is extracted from the Extension Payload.
2. The Timestamp Payload is checked, and the message is discarded if the counter is larger or equal to the current MIKEY replay counter associated with the given MSK (the 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 RFC 1982 [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********

6.5.2 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~~EXT. If the key in the message is an MSK protected by MUK, MGV-F retrieves the MUK identified as specified in clause 6.1.~~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~~EXT. If the key inside the message is an MTK protected by MSK, 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).].

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

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].

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

Annex D (normative): UICC-ME interface

D.1 MSK Update Procedure

This procedure is part of the MSK update procedure as described in clause 6.5 (Validation and key derivation functions in MGV-F).

The ME has previously performed a GBA_U bootstrapping procedure as described in TS 33.220. The UICC stores the corresponding Ks_int_NAF together with the NAF_Id associated with this particular bootstrapping procedure.

The ME receives a MIKEY message containing an MSK update procedure. After performing some validity checks, the ME sends the whole message to the UICC. The ~~ME~~ UICC ~~also includes in this request NAF_Id~~uses the MUK ID (included in the MIKEY message, see clause 6.1) to identify the stored Ks_int_NAF.

The UICC then uses Ks_int_NAF as the MUK value for MUK derivation and MSK validation and derivation (as described in clause 6.5.3).

After successful MSK Update procedure the UICC stores the ~~Network~~ Key Domain ID~~, Key Group ID~~, MSK ID, MSK and MSK Validity Time (in the form of MTK ID interval).

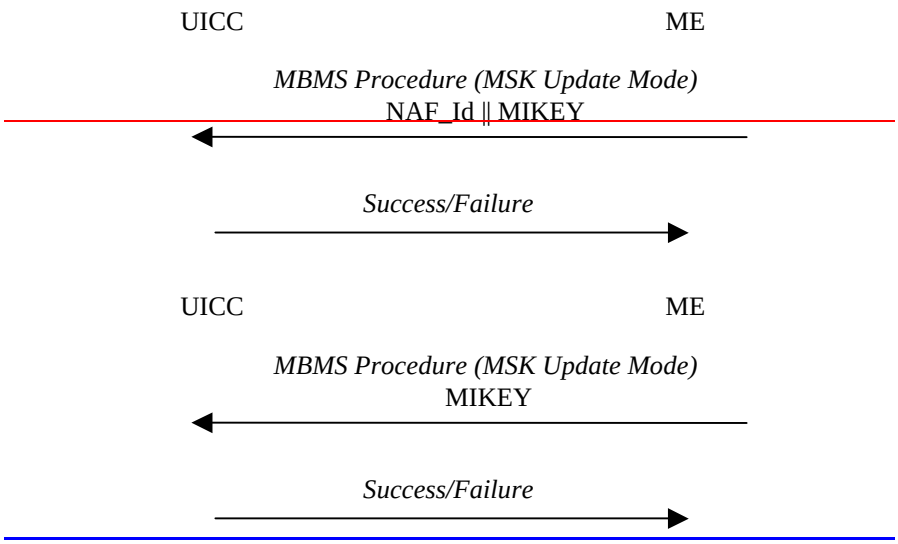


Figure D.1: MSK Update Procedure

D.2 MSK Verification Message Generation

This procedure is part of the MSK Verification Message as described in clause 6.4.5.2 (MSK Verification message).

The ME constructs the verification message in response to the MSK-transport message when it is required by BM-SC.

The ME shall then give the constructed MIKEY verification message, with an empty MAC field, to the UICC and the ME shall include NAF_id in this message. The ~~ME~~ UICC ~~also includes in this request NAF_Id~~ uses the MUK ID (see clause 6.1) to identify the stored Ks_int_NAF=MUK to be used in the MSK Verification Message Generation.

The UICC will verify that the Time Stamp MIKEY field correspond to the previous MSK Update procedure. Then, the UICC shall compute and send the MIKEY packet to the ME (including the calculated MAC field) as defined in clause 6.4.5.2. (MSK Verification message).

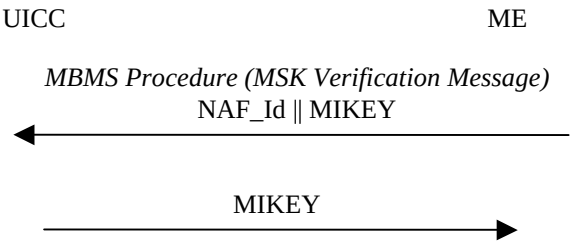


Figure D.2: MSK Verification Message

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

D.3 MTK generation and validation

This procedure is part of the MTK generation and validation function as described in clause 6.5.4 (MTK validation and derivation).

The ME receives the MIKEY message (containing Header, Time stamp, ~~Network~~ Key Domain ID~~, Key Group ID~~, MSK ID, MTK ID = SEQp, MSK_C[MTK] and MAC). After performing some validity checks, the ME sends the whole message to the UICC. The UICC computes the MGV-F function as described in clause 6.5. (Validation and key derivation functions in MGV-F). After successful MGV-F procedure the UICC returns the MTK.

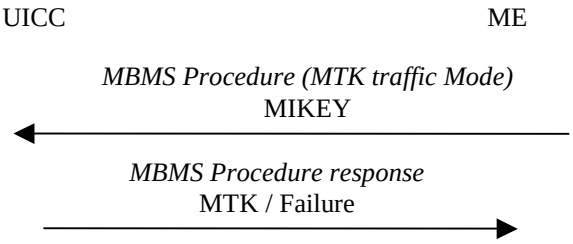


Figure D.3: MTK Generation and Validation