**3GPP TSG SA WG3 Security ó SA3#36** **S3-041041**

**November 23 - 26, 2004** **(comments to S3-041017)**

**Shenzen, China**

**Title:** **Update of** S3-041017: **Key group ID and MSK ID**

**Source:** **Ericsson**

**Document for:** **Discussion and decision**

**Agenda Item:**

**Work Item:** **MBMS**

# 1 Introduction

This contribution studies if Key group ID can be merged to MSK ID and how the key IDs are carried in MSK and MTK messages.

# 2 Discussion

## 2.1 Combining Key group ID and MSK ID

Current TS 33.246 [1] identifies MSK keys as follows 6.3.2.1:

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

*where*

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

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

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

There are some reasons why Key Group ID should be merged to MSK ID.

1. The Key Group ID is always related to MSK ID. There seems to be no functional reason why these should be carried separately.

2. Carrying Key Group ID and MSK ID together clarifies the usage of keys in MBMS. The relation between Key Group ID and MSK ID becomes evident.

3. Carrying Key Group ID in the CSB field of MIKEY [2] is not semantically correct according to RFC 3830 since the CSB-ID field should identify the key material that was used to protect the MIKEY

message, i.e. the ìouter key IDî in MBMS terms. Currently in MTK messages CSB ID carries only part of that information and in MSK messages it carries part of ìinner key IDî.

4. MIKEY verification message includes also CSB ID field. Carrying Key Group ID in MSK verification message CSB ID field is unnecessary since it does not help identify the key, i.e. MUK, that was used to protect the verification message. This hints that MUK ID should be carried in CSB ID field of MSK messages, if possible.

5. The 2 byte Key Group ID is carried in 4 byte CSB ID field. This means that two bytes of are unused (i.e. wasted) in each MIKEY message. If Key Group ID is combined to MSK ID the result will be 4 bytes ID that will fit to CSB ID.

Therefore it is proposed to merge Key Group ID with MSK ID. The new ID could be a 4 byte concatenation Key Group ID with MSK ID. The meaning of the fields would be the same earlier. It is proposed to define the *new MSK ID* as follows:

MSK ID = (Service ID part || Key ID part) where

Service ID part is 2 bytes long and is used to group keys together in order to allow redundant MSKs to be deleted.

Key ID part is 2 bytes long and is used to distinguish MSKs that have the same Network ID and Service ID.

## 2.2 Carrying MTK ID and new MSK ID in MTK messages

It is proposed that the key IDs are carried in MTK message as follows:

- The new MSK ID (4 bytes) is carried in the CSB field of the common header. This identifies the ìouter keyî in MTK message.

- The MTK ID (2 bytes) is carried in the extension payload. This identifies the ìinner keyî in MTK message. Carrying only one key ID is possible according to the internet draft on MBMS extensions to MIKEY RFC, see another contribution from Ericsson.

This follows the semantics of RFC 3830 and saves 2 bytes for each MTK message since the new MSK ID fits exactly to CSB ID field.

## 2.3 Carrying MUK ID and new MSK ID in MSK messages

The MUK ID has not been defined yet, thus there are different alternatives how to carry the MUK ID and the new MSK ID in the MSK message. It should be noted that also the verification message needs to be taken into account.

**1.** The most natural way is to carry the MUK ID in the CSB ID field and MSK ID in the extension header, i.e. **the MSK message** looks like:

- The MUK ID is carried in the CSB field of the common header. This identifies the ìouter keyî in MSK message.

- The MSK ID (4 bytes) is carried in the extension payload. This identifies the ìinner keyî in MSK message. Carrying only one key ID is possible according to the internet draft on MBMS extensions to MIKEY RFC, see another contribution from Ericsson.

The **MSK verification message looks** like:

- The MUK ID is carried in the CSB field of the common header. This identifies the ìouter keyî in MSK verification message.

- The MSK ID (4 bytes) does not need to be carried in the verification message.

This alternative requires that MUK ID fits into the CSB ID field. A proposal for MUK ID is presented in another Ericsson contribution.

**2.** If the MUK ID does not fit into the CSB ID field, it is possible to carry both MUK ID and MSK ID in the new extension payload, i.e. **the MSK message** looks like:

- The MUK ID is carried in the extension payload. This identifies the ìouter keyî in MSK message.

- The MSK ID (4 bytes) is carried in the extension payload. This identifies the ìinner keyî in MSK message. Carrying also two key IDs is possible according to the internet draft on MBMS extensions to MIKEY RFC, see another contribution from Ericsson.

The **MSK verification message looks** like:

- The MUK ID is carried in the extension payload. This identifies the ìouter keyî in MSK message.

- The MSK ID (4 bytes) does not need to be carried in the verification message.

This alternative has the drawback that it leaves CSB ID field empty in both directions and the use of CSB ID field is against the semantics of RFC 3830.

**3.** If the MUK ID does not fit into the CSB ID field and in order to use the CSB ID field, it is possible to carry MUK ID in the new extension payload and MSK ID in the CSB field. The use of CSB ID field is against the semantics of RFC 3830 but it would save 4 bytes, i.e. **the MSK message** looks like:

- The MSK ID (4 bytes) is carried in the CSB field of the common header. This identifies the ìinner keyî in MSK message. This identifies the ìinner keyî in MSK message. Carrying also two key IDs is possible according to the internet draft on MBMS extensions to MIKEY RFC, see another contribution from Ericsson.

- The MUK ID is carried in the extension payload. This identifies the ìouter keyî in MSK message.

The **MSK verification message looks** like:

- The MSK ID (4 bytes) does not need to be carried in the verification message, but the CSB ID field can carry it.

- The MUK ID is carried in the extension payload. This identifies the ìouter keyî in MSK verification message.

This alternative has the drawback that it leaves CSB ID field empty in the MSK verification message and the use of CSB ID field is against the semantics of RFC 3830.

# 3 Conclusions and proposal

In order to clarify the usage of key identities and to align with RFC 3830, this contribution has proposed to combine Key Group ID and MSK ID into a new MSK ID that would be MSK ID = (Service ID part || Key ID part). The semantics of the Service ID part remains the same as the old Key group ID and the semantics of the Key ID part is the same as the old MSK ID.

This contribution analysed how to carry MUK ID, new MSK ID and MTK ID in MIKEY messages. This should be aligned with MIKEY RFC 3830.

- It is proposed that alternative 1 is chosen for the **MSK message**. I.e. MSK message carries MUK ID in CSB ID field and new MSK ID in extension payload. This is according to semantics of CSB field in RFC 3830 and it does not send empty fields. This proposal depends on the decision on MUK ID, see other contribution from Ericsson. If MUK ID is too long to be carried in the CSB ID field, it is proposed to choose alternative 3.

- It is also proposed that MTK message carries new MSK ID in CSB ID field and MTK ID in extension payload.

CRs from Ericsson to this meeting propose needed changes in TS 33.246.

# 4 References


[1] TS 33.246, Security of MBMS

[2] RFC 3830, MIKEY

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

***Tdoc ⌘Att1_S3-041041***

*CR-Form-v7*

# CHANGE REQUEST

⌘ **33.246** **CR** **008** ⌘**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 Key processing (updated according to S3-041017) |
| ***Source:*** | ⌘ | Ericsson |
| ***Work item code:*** | ⌘ | MBMS |
| ***Date:*** | ⌘ | 15/11/2004 |
| ***Category:*** | ⌘ | **C** |
| ***Release:*** | ⌘ | Rel-6 |

*Use one of the following categories:*
***F*** *(correction)*
***A*** *(corresponds to a correction in an earlier release)*
***B*** *(addition of feature),*
***C*** *(functional modification of feature)*
***D*** *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*

| | |
|---|---|
| *2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |

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

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 6.4.1, 6.4.2, 6.5.2, 6.5.3, 6.5.4 |

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

| | | |
|---|---|---|
| ***Other comments:*** | ⌘ | |

# 2 References

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

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

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


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

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

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

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

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

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

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

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

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

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

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

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

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


__FIRST_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 contains the key types and identities of MSKs and the MTKs (see clause 6.3.2 and 6.3.3).

### 6.4.2 MIKEY common header

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

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

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

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

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

The CSB ID field of MIKEY common header shall carry the MUK ID in MSK key update messages and MSK ID in MTK key update messages ~~Key Group ID~~.

## __SECOND_CHANGE__

### 6.5.2 MUK derivation

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

### 6.5.3 MSK processing~~validation and derivation~~

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

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

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

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

### 6.5.4 MTK processing~~validation and derivation~~

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the ~~Data Type field in the common header~~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).].

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

***Tdoc ⌘Att2_3-041041***

*CR-Form-v7*

# CHANGE REQUEST

⌘ **33.246** **CR** **013** ⌘**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:*** | ⌘ | Alignment of Key ID place holders with MIKEY (this is an update according to S3-041017) |
| ***Source:*** | ⌘ | Ericsson |
| ***Work item code:*** | ⌘ | MBMS |
| ***Date:*** | ⌘ | 18/11/2004 |
| ***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:*** | ⌘ | Carrying Key group ID in CSB ID field of MIKEY is not according to semantics of the CSB field. The ID of the key that was used protect the message should be carried in CSB field. This means MUK ID in MSK messages and MSK ID in MTK messages. Especially, in MSK verification message there is no need to carry the Key Group ID in CSB ID field since it does not identify the MUK. It is proposed to align the usage of fields according to MIKEY RFC<br>Also, there seems to be no need to have separate Key group ID and MSK ID. It is proposed to combine these to a new MSK ID which has two parts with the same meaning as the Key Group ID and MSK ID had. |
| ***Summary of change:*** | ⌘ | Key group ID and MSK ID are combined to a new MSK ID which has two parts with the same meaning as the Key Group ID and MSK ID had.<br><br>The key IDs are carried as follows:<br>• For MSK messages: MUK ID is in CSB ID field and MSK ID is in extension payload.<br>• For MTK messages: MSK ID is in CSB ID field and MTK ID is in extension payload. |
| ***Consequences if not approved:*** | ⌘ | The placement of key IDs deviates unnecessarily from MIKEY RFC 3830.<br>MSK verificaiton message needs to carry the extension payload to identify the MUK. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 2, 6.3.2.1, 6.3.3.1, 6.4.4, 6.4.5, 6.4.5.0 (removed), 6.4.5.1, 6.4.5.1.1 (removed), 6.4.5.3, 6.4.5.3.1 (removed), 6.4.6.1, 6.4.6.2, 6.6.2.1, D.1, D.3 |

| | | Y | N | | | |
|---|---|---|---|---|---|---|
| ***Other specs affected:*** | ⌘ | 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**********

### 6.3.2.1 MSK identification

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

where

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

MSK ID = (Service ID part || Key ID part) where

Service ID part ~~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.~~

Key ID part ~~MSK ID~~ is 2 bytes long and is used to distinguish MSKs that have the same Network ID and Service ID part. Value 0x0 shall be used to denote the current MSK.~~Key Group ID~~. ~~It is carried in the MSK ID field of MIKEY extension payload.~~

The MSK ID is carried in the extension payload in MSK key update messages and in CSB ID field in MTK key update messages.

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

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

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

## 6.4.4 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in RFC 3830 [9] (MIKEY). To be able to keep track of the key~~s~~ that is delivered in the message, a ~~new~~ general Extension Payload (EXT) is ~~defined~~ used that conforms to the structure defined in [13] ~~section 6.15 of RFC 3830 [9] (MIKEY)~~.

~~For MBMS the general extension payload (according to table 6.15 of [9]) shall be identified by following value:~~

| ~~Type~~ | ~~Value~~ | ~~Comments~~ |
|---|---|---|
| ~~3GPP MBMS~~ | ~~x~~ | ~~3GPP extension payload for MBMS key management~~ |

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

The type and ID~~s~~ of the ~~involved~~ key~~s~~ that is delivered in the message ~~are~~ is ~~kept~~ carried in the EXT. This EXT is incorporated in the MIKEY messages (see Figure 6.4).~~, to enable the UE to look up t~~The identity of the key, which was used to protect the message is carried in CSB ID field of the common header~~, and which key is delivered in the message~~. ~~This EXT is incorporated in the MIKEY messages (see Figure 6.4).~~

When a~~n~~ MIKEY message ~~MSK~~ is delivered to a UE, ~~the~~it ~~MIKEY message~~ contains an ~~EXT~~ Extension Payload that ~~holds~~ includes Type field value x.

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

The CSB ID field identifies the outer key ID that is the ID of the key used as pre-shared secret for the key delivery (i.e. an MUK or MSK). The EXT include a Key Type ID sub-payload as defined in [13]. It identifies the inner key ID that is transported in the message (i.e. an MSK or MTK). For messages that contain an MSK, the CSB ID field includes the MUK ID of the MUK used to protect the delivery, and the Key Type ID subpayload includes the Key Type and MSK ID of the MSK delivered in the message. For messages that contain an MTK, the CSB ID field includes ~~EXT contains~~ the MSK ID of the MSK used to protect the delivery, and the Key Type ID subpayload includes the Key Type and

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.

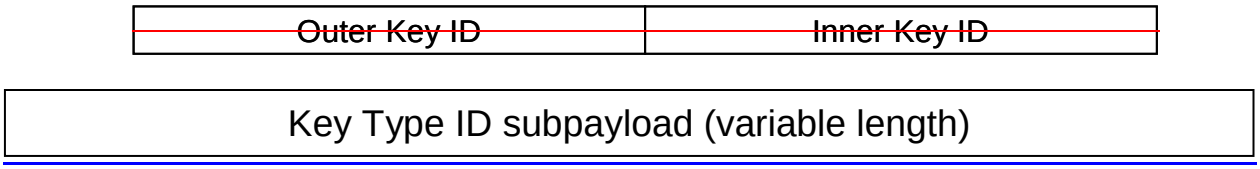



**Figure 6.4: Extension payload used with MIKEY**

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).

## 6.4.5 MIKEY message structure

### 6.4.5.0 MSK and MTK transport identification

For MBMS the MIKEY common header data type field (cf. Table 6.1a of clause 6.1 [9]) identifies the type of key that is transported.

The transport of MSK and MTK transport shall be identified by following values:

| Data type | Value | Comment |
|---|---|---|
| MSK | x | Transport of MSK encrypted with MUK |
| MTK | x | Transport of MTK encrypted with MSK |

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

### 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 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 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.

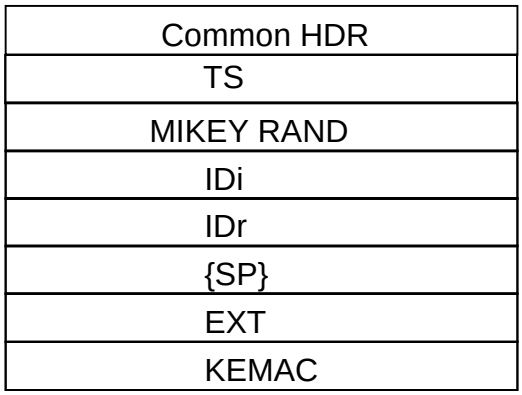



**Figure 6.5: The logical structure of the MIKEY message used to deliver MSK.**
**For use of brackets, cf. section 1.3 of RFC 3830 [9] (MIKEY)**

~~6.4.5.1.1 Key Data Sub payloads carried by KEMAC~~

~~For MBMS MSK transport, the Key Data Sub payload (cf. clause 6.13 of [9]) that is carried by the KEMAC payload shall be identified by following value:~~

~~Data type | Value | Comment~~

~~MSK | x | MSK encrypted with MUK~~

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

********** NEXT 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. The network identity payloads (IDi) shall be used in MTK transport messages.

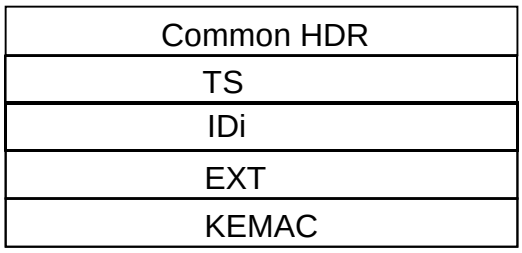



**Figure 6.7: The logical structure of the MIKEY message used to deliver MTK**

~~6.4.5.3.1 Key Data Sub payloads carried by KEMAC~~

~~For MBMS MTK transport, the Key Data Sub payload (cf. clause 6.13 of [9]) that is carried by the KEMAC payload shall be identified by following value:~~

~~Data type | Value | Comment~~

~~MTK | x | MTK encrypted with MSK~~

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

********** 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 extracted from the ~~Extension Payload~~CSB ID field.
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~~CSB ID field.
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********

### 6.6.2.1 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********

# 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 also includes in this request NAF_Id 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 ID~~, Key Group ID~~, MSK ID, MSK and MSK Validity Time (in the form of MTK ID interval).

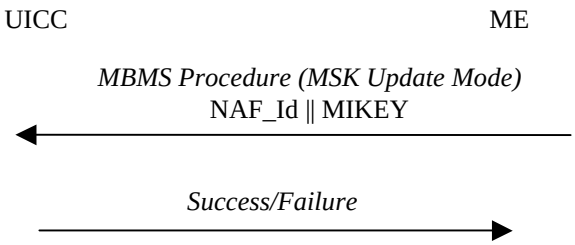



**Figure D.1: MSK Update Procedure**

******** 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 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.

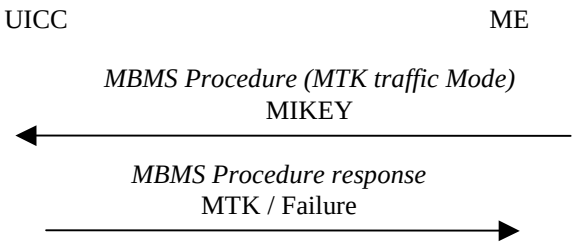



**Figure D.3: MTK Generation and Validation**

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

***Tdoc ⌘Att3_S3-041041***

*CR-Form-v7*

# CHANGE REQUEST

⌘ **33.246** **CR** **021** ⌘ **rev** **6** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

***Proposed change affects:*** UICC apps⌘ ☐ ME [X] Radio Access Network ☐ Core Network [X]

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Clarification of MSK key management (updated according to S3-041017) |
| ***Source:*** | ⌘ | Ericsson |
| ***Work item code:*** | ⌘ | MBMS |
| ***Date:*** | ⌘ | 15/11/2004 |
| ***Category:*** | ⌘ | **C** |
| ***Release:*** | ⌘ | Rel-6 |

*Use one of the following categories:*
***F*** *(correction)*
***A*** *(corresponds to a correction in an earlier release)*
***B*** *(addition of feature),*
***C*** *(functional modification of feature)*
***D*** *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*
*2 (GSM Phase 2)*
*R96 (Release 1996)*
*R97 (Release 1997)*
*R98 (Release 1998)*
*R99 (Release 1999)*
*Rel-4 (Release 4)*
*Rel-5 (Release 5)*
*Rel-6 (Release 6)*

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

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

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

***Other comments:*** ⌘

# 2 References

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

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

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


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

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

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

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

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

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

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

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

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

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

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

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

[13] 3GPP TS 26.346: "MBMS, Protocols and codecs".


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

## 6.3.2 MSK procedures

### 6.3.2.1 MSK identification

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

where

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

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

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

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

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

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

#### 6.3.2.2.1 Basic MSK retrieval procedure

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

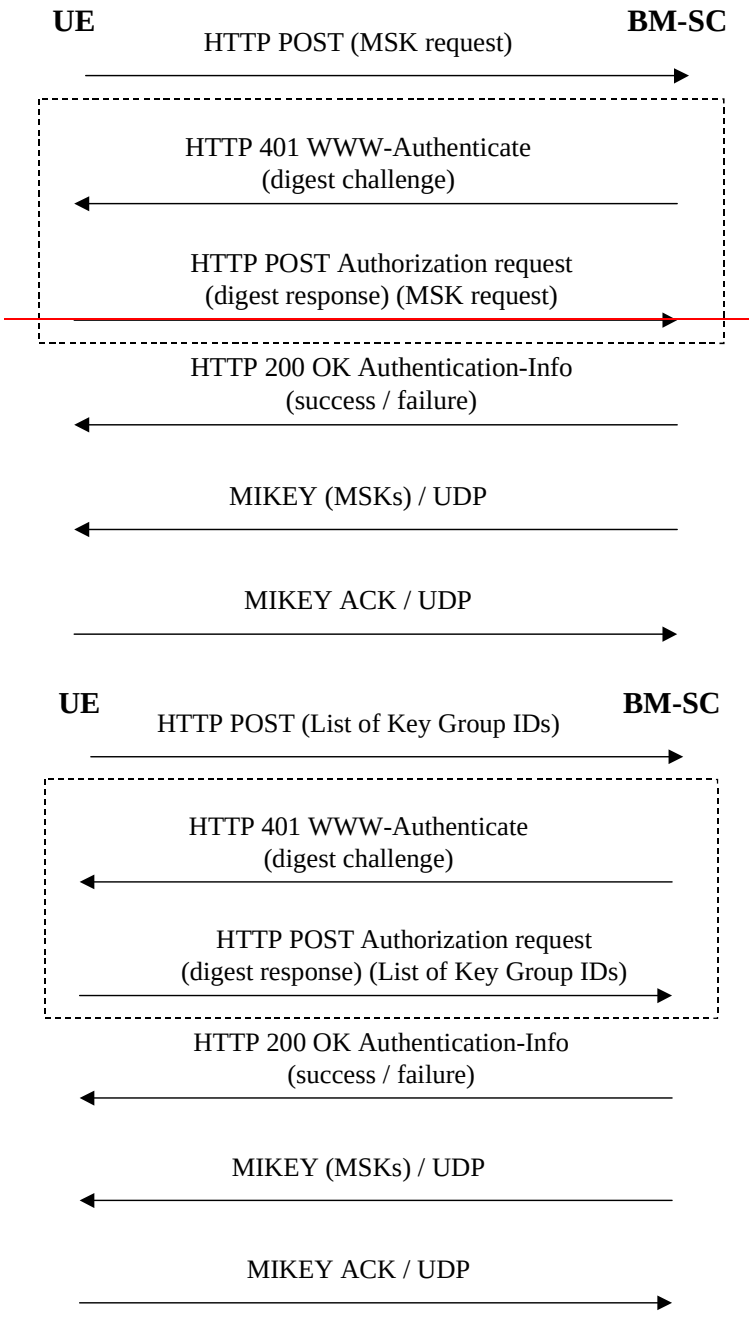



**Figure 6.1: ~~UE initiated MSK delivery~~Basic MSK retrieval procedure**

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

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

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

NOTE: When the Key ID part of the MSK ID~~(s) are~~ is set to 0x0, this means the current MSK, see clause 6.3.2.1~~not needed in the request since BM-SC will send the current valid MSK for each Key Group ID~~.

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.~~

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

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:

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

~~NOTE:~~ The Key ID part of the MSK ID(s) shall be set to 0x0 to denote the current MSK. Specific Key ID values are not used since they may change over time and ~~Key Group ID~~Service ID 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.

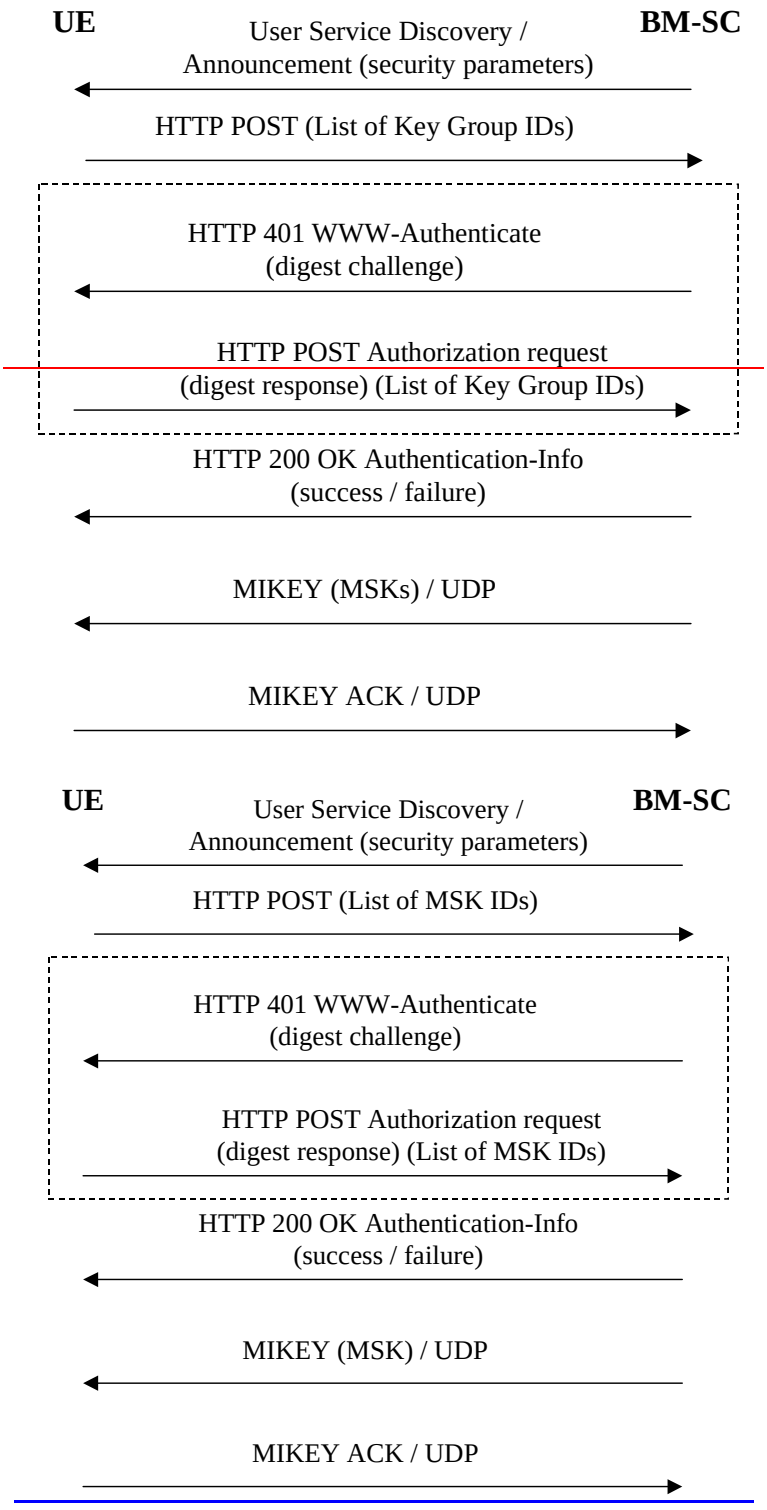



**Figure 6.x: MSK retrieval procedure**

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

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

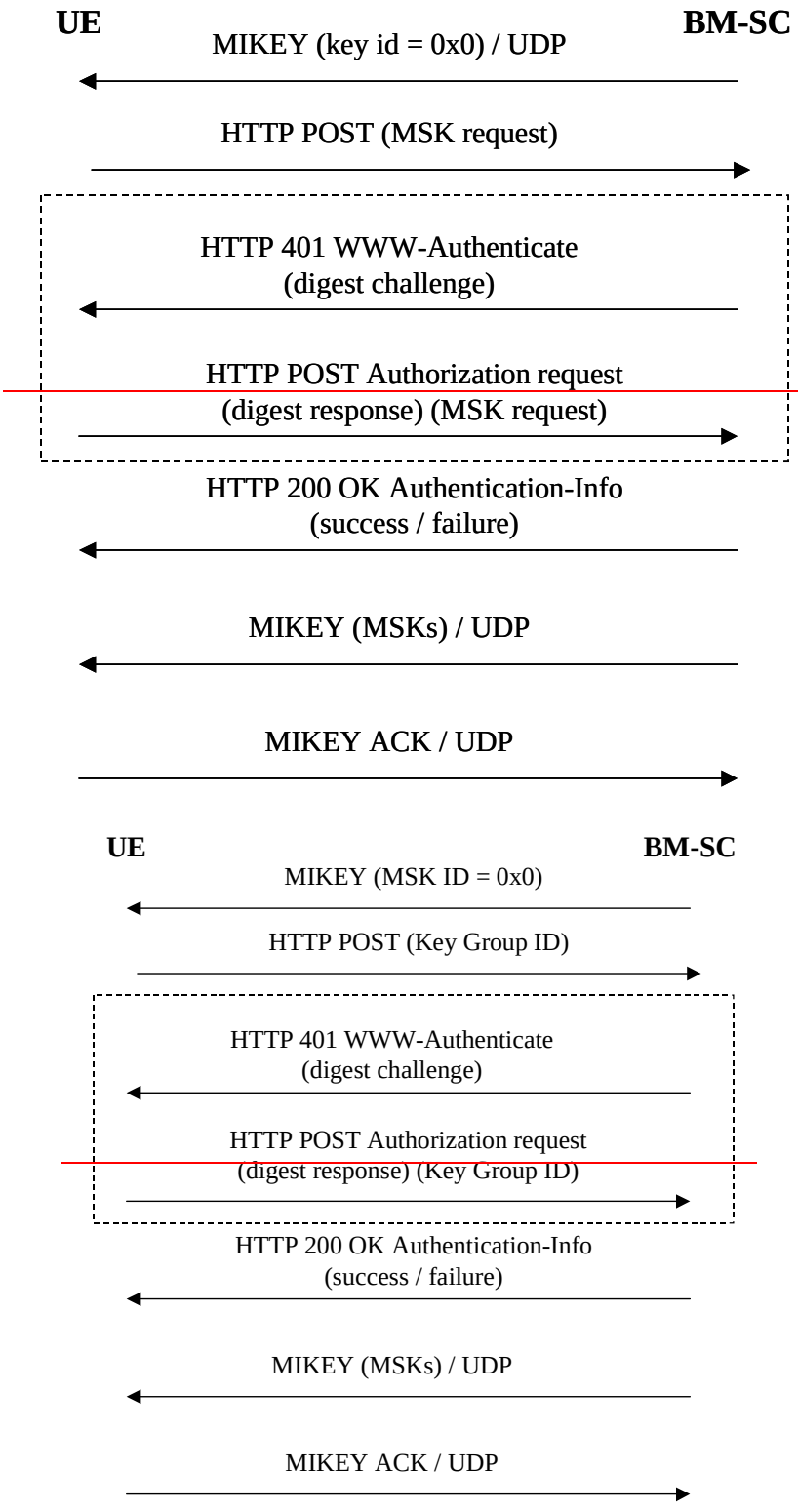
The rest of the procedure is the same as in 6.3.2.3.1.

#### 6.3.2.2.3 Missed key update procedure

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

#### 6.3.2.2.4 BM-SC solicited pull

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


UE
BM-SC
MIKEY (key id = 0x0) / UDP
HTTP POST (MSK request)
HTTP 401 WWW-Authenticate
(digest challenge)
HTTP POST Authorization request
(digest response) (MSK request)
HTTP 200 OK Authentication-Info
(success / failure)
MIKEY (MSKs) / UDP
MIKEY ACK / UDP
UE
BM-SC
MIKEY (MSK ID = 0x0)
HTTP POST (Key Group ID)
HTTP 401 WWW-Authenticate
(digest challenge)
HTTP POST Authorization request
(digest response) (Key Group ID)
HTTP 200 OK Authentication-Info
(success / failure)
MIKEY (MSKs) / UDP
MIKEY ACK / UDP

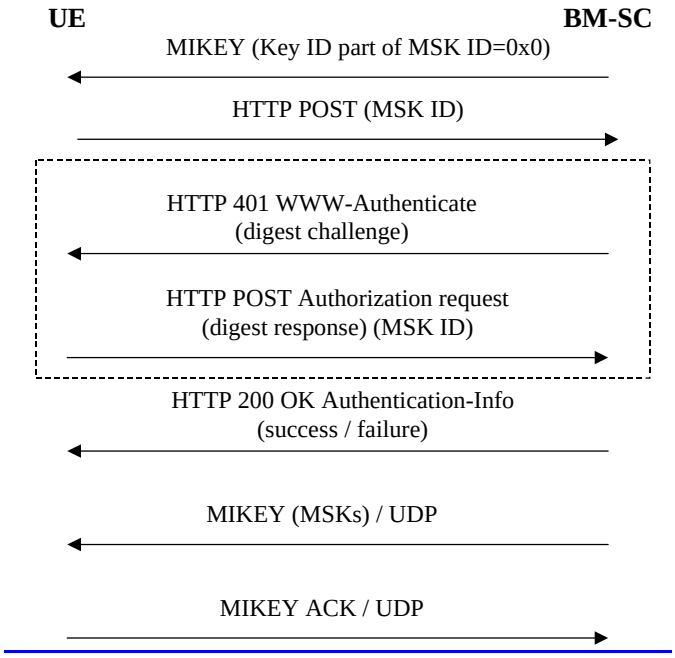



**Figure 6.3: BM-SC solicited pull**

The BM-SC sends MIKEY message over UDP to the UE. The Key ID 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: 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~~Service ID. 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.

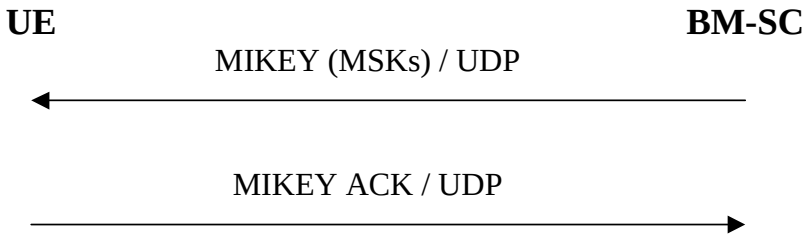


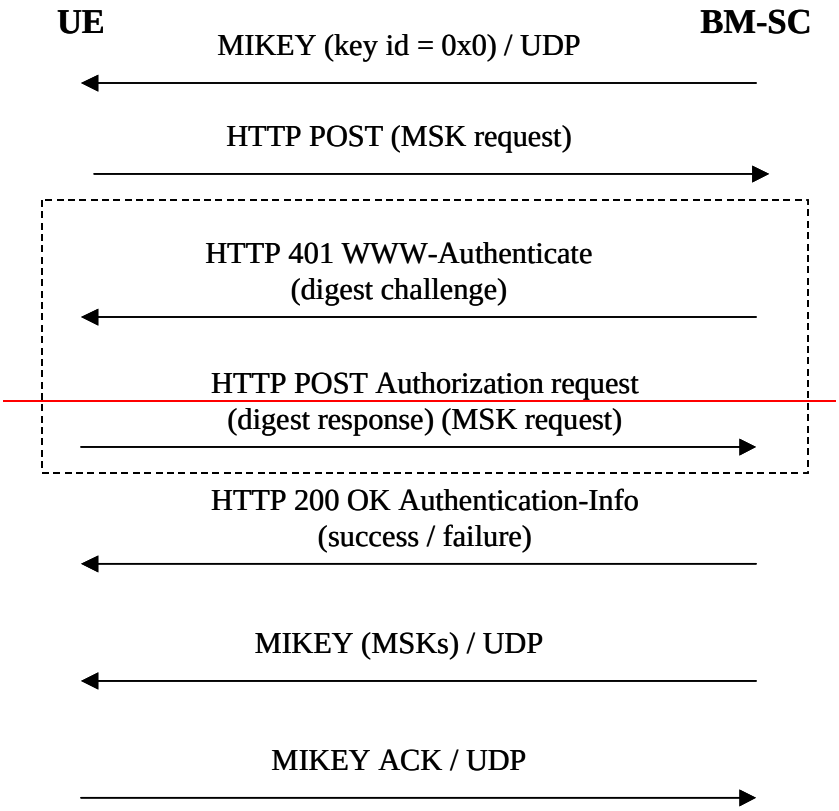

**Figure 6.2: Pushing the MSKs to the UE**

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.~~