**3GPP TSG SA WG3 Security — SA3#36** **S3-040996**

**November 23 - 26, 2004**

**Shenzhen, China**

| | |
|---|---|
| **Title:** | **MUK ID and UE ID in MBMS** |
| **Source:** | **Ericsson** |
| **Document for:** | **Discussion and decision** |
| **Agenda Item:** | **6.20** |
| **Work Item:** | **MBMS** |

# 1 Introduction

The MBMS User Key (MUK) is identified by MUK ID in MIKEY MSK message in TS 33.246 [1]. The format of MUK ID is not currently specified. This contribution discusses different alternatives for MUK ID and proposes that a hash of (B-TID || NAF ID) is used as MUK ID.

# 2 Discussion

## 2.1 Background

MBMS User Key (MUK) is used to protect the MSK delivery from BM-SC to the UE and the corresponding acknowledgement message. MUK is specific to one UE – BM-SC (i.e. NAF) pair. MUK is derived from NAF specific GBA key, i.e. from Ks_int_NAF or Ks_NAF, depending if GBA_U or GBA_ME is used. It should be noted that GBA key Ks is identified by B-TID (base64encoded(RAND)@BSF_name), but identifiers for NAF specific GBA keys have not been specified.

## 2.2 MUK ID

Using NAF-ID alone as MUK-ID is not enough as it could lead to some errors for MIKEY push based handling. Suppose the case that the UE receives a MIKEY message. That message needs to be protected by the last valid MUK. If the UE has already done a bootstrapping and replaced the MUK, but the new B-TID did not reach the BM-SC. Thus the UE is not able to distinguish the old and new MUK if only NAF ID is used.

The analysed alternatives are presented in Table 1.

Alternative 1.
There are several alternatives for MUK ID. An obvious identifier for MUK ID would be a combination of B-TID and NAF ID. However, this is unnecessarily long. A simpler version for MUK ID could be base64encoded(RAND)@NAF ID. Collisions of RAND in UE should not be possible since the RAND is received from home HSS. There is a small probability of RAND collisions in BM-SC. This is avoided if the BM-SC stores the MUKs with some other index information than MUK-ID, e.g. with IMSI. This is because

otherwise the BM-SC is not able to replace the old MUK with a new one when a new GBA is run. Therefore base64encoded(RAND)@NAF ID is proposed as the starting point of MUK ID. Alternative 1 has two variations. 1a is the one described above. 1b is the same as 1a but the NAF ID is already present, e.g. in IDi field of MIKEY. In this case NAF ID is not needed in MUK ID. This is analysed as alternative 2b below.

Alternative 2.
Alternative 2 has two variations. In 2b NAF ID is already present in message. The MUK-ID may therefore be shorter and include only the base64encoded (RAND). The same notes on collision apply as in 1a. Alternative 2a is not considered since the NAF-ID is not present and UE cannot distinguish different BM-SCs. (NAF ID is not currently present in MIKEY message, see other Ericsson contribution on the issue.)

Alternative 3.
The length of RAND is 16 bytes. It may be beneficial to have shorter MUK ID to save storage space in the BM-SC and in the air interface although MSK updates should be relatively rare. In alternative 3 a hash of B-TID | NAF_ID is used as MUK ID.

In 3a the NAF ID is not present in the message. In BM-SC there is no risk of collisions between two UEs for the same reason as in alt 1. A risk is for collisions between consecutive MUKs for the same UE. In UE there is a risk that hashes for two BM-SCs collide. Also there is risk is for collisions between consecutive MUKs for the same BM-SC. A possible solution for collisions could be that if collisions occur in UE between two MUKs, the UE should run new GBA procedure to get a new B-TID. This would be a recovery procedure for a case that is assumed to be rare anyway.

In 3b the only collision risks are for consecutive MUKs.

| Alternative | MUK ID | If NAF ID present anyway (e.g. in IDi) | Comment |
|---|---|---|---|
| 1a | base64enc(RAND)@NAF_ID | N.A | Quite long. No collision risks if MUK-ID indexed with e.g. IMSI |
| 1b | base64enc(RAND)@NAF_ID | NAF_ID | See 2b |
| 2a | base64enc(RAND) | N.A | Not applicable |
| 2b | base64enc(RAND) | NAF_ID | Shorter MUK-ID than in 1a. No collision risks if MUK-ID indexed with e.g. IMSI. Requires NAF ID in IDi. |
| 3a | Hash(B-TID \| NAF_ID) | N.A | MUK-ID can be short. Collision risks for two BM-SCs and consecutive MUKs. |
| 3b | Hash(B-TID \| NAF_ID) | NAF_ID | MUK-ID can be short. Collision risks for consecutive MUKs. |

Note that the chosen alternative should be included also in the MSK verification message (if that was requested by the BM-SC). Currently the verification message does not carry the extension header field.

## 2.3 UE ID

The MIKEY messages carrying MSK include currently IDr field and the TS specifies this to identify the UE in question. However, since the MUK ID will identify the UE uniquely and because the IDr is optional field in MIKEY RFC 3830 [2], the IDr field is not needed in MBMS. Therefore it is proposed to remove the IDr field in the TS and add a clarifying note why it is not needed.

# 3 Stage 3 impacts

It should be noted that the MUK ID means impacts to stage 3 terminal specifications, e.g. in TS 31.102. However, MUK ID has not been specified until now, thus impacts seem inevitable. Also, TS 31.102 seems to require updates anyway since it currently uses NAF ID instead of MUK ID in identifying the MUK.

Also TS 33.246 includes a contradiction in this issue.

Chapter 6.5.3 states: *When the MGV-F receives the MIKEY message, it first determines the type of message by reading the Data Type field in the common header. If the key in the message is an MSK,* ***MGV-F retrieves the MUK with the ID given by the Extension payload.***

Annex D.1 states in turn: *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).*

# 4 Conclusions and proposal

Different alternatives for MUK ID were analysed. Some of them require that NAF ID is carried in IDi field of MIKEY.

1a. base64enc(RAND)@NAF_ID

2b. base64enc(RAND), requires that NAF ID is carried in IDi field

3a. hash(B-TID | NAF_ID) without NAF ID in IDi

3b. hash(B-TID | NAF_ID) with NAF ID in IDi

Alternatives 3a and 3b are preferred since they require less storage space in BM-SC. Hash collisions can be recovered by so that the UE runs a new GBA run if a collision occurs. It is proposed that 3a is adopted since it is simpler by not requiring existence of NAF ID in IDi.

An attached CR from Ericsson to this meeting proposes needed changes in TS 33.246.

# 5 References

[1] TS 33.246, Security of MBMS

[2] IETF RFC 3830, MIKEY: Multimedia Internet Keying

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

***Tdoc ⌘Att1_S3-040996***

*CR-Form-v7*

# CHANGE REQUEST

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ⌘ | **33.246** | **CR** | **024** | ⌘**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 ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | MUK ID in MBMS | | |
| ***Source:*** | ⌘ | Ericsson | | |
| ***Work item code:*** | ⌘ | MBMS | ***Date:*** ⌘ | 12/11/2004 |
| ***Category:*** | ⌘ | **C** | ***Release:*** ⌘ | Rel-6 |
| | | *Use one of the following categories:*<br>***F*** *(correction)*<br>***A*** *(corresponds to a correction in an earlier release)*<br>***B*** *(addition of feature),*<br>***C*** *(functional modification of feature)*<br>***D*** *(editorial modification)*<br>Detailed explanations of the above categories can be found in 3GPP TR 21.900. | *Use one of the following releases:*<br>*2 (GSM Phase 2)*<br>*R96 (Release 1996)*<br>*R97 (Release 1997)*<br>*R98 (Release 1998)*<br>*R99 (Release 1999)*<br>*Rel-4 (Release 4)*<br>*Rel-5 (Release 5)*<br>*Rel-6 (Release 6)* | |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | MUK ID has not been defined. |
| ***Summary of change:*** | ⌘ | MUK ID shall be a four byte hash of (B-TID \|\| NAF ID). How MUK ID is carried in MIKEY is desctibed in another CR from Ericsson. |
| ***Consequences if not approved:*** | ⌘ | MUK ID remains unspecified. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | | | | | |
| | | Y | N | | | |
| ***Other specs affected:*** | ⌘ | X | | Other core specifications | ⌘ | TS 31.102 |
| | | | X | Test specifications | | |
| | | | X | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

## 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 identifed with MUK ID, where MUK ID is defined as hash(B-TID || NAF_ID), where the hash function is is four most significant bytes from SHA1. B-TID and NAF_ID are defined as specified in TS 33.220 [6]. Both MGV-F and BM-SC shall calculate the MUK ID.

NOTE: The BM-SC shall store the MUKs per UE, e.g. using IMSI an index. I.e. it shall not use the MUK ID as index when storing the MUKs of different UEs. Otherwise the BM-SC is not able to update the old MUK with new MUK when the MUK is updated.

The UE shall check whether the hash collides with any other MUK ID. If it does, the UE shall run a new bootstrapping procedure.

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

## 6.4.5 MIKEY message structure

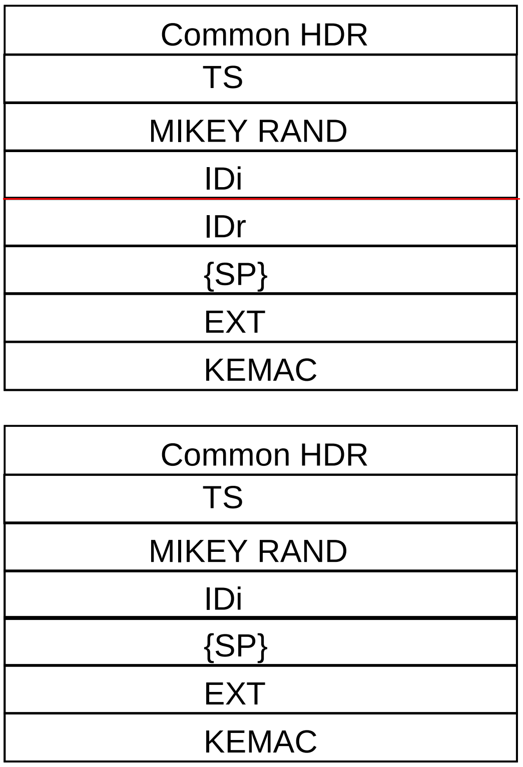
### 6.4.5.1 MSK message structure

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 payload~~s~~ 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).

NOTE: The usage of IDr payload is optional in RFC 3830. Since the MUK ID identifies the UE uniquely, the IDr payload is not needed in MBMS.

~~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.



Common HDR
TS
MIKEY RAND
IDi
IDr
{SP}
EXT
KEMAC

Common HDR
TS
MIKEY RAND
IDi
{SP}
EXT
KEMAC

**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 IDs 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.

NOTE: The usage of IDr payload is optional in RFC 3830. Since the MUK ID identifies the UE uniquely, the IDr payload is not needed in MBMS.

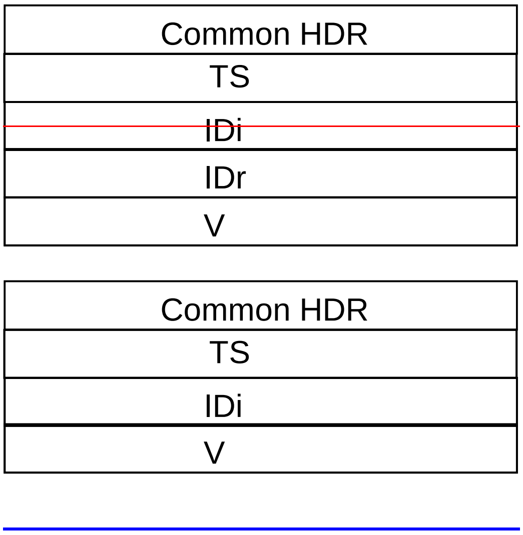


Figure 6.6: The logical structure of the MIKEY Verification message

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*********

# 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 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).

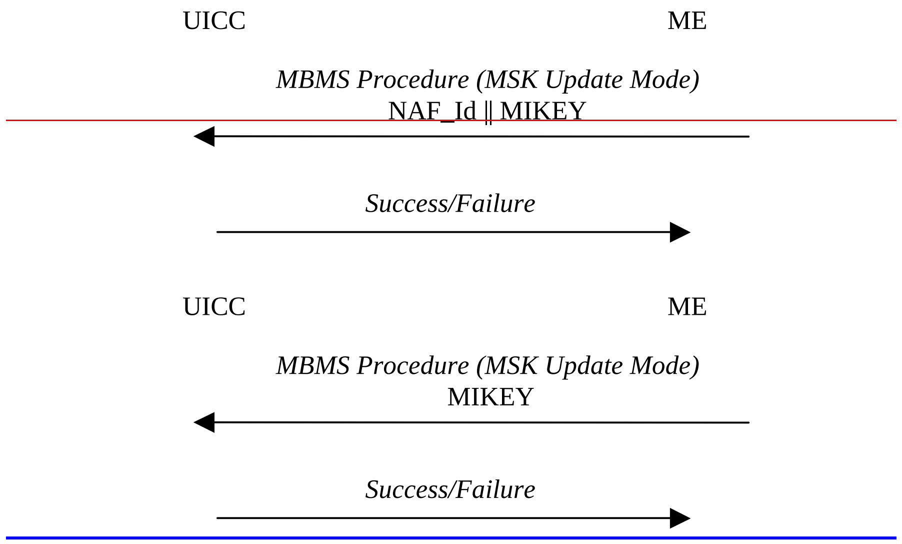


**Figure D.1: MSK Update Procedure**

# 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. The ~~ME~~ UICC ~~also includes in this request NAF_Id~~ uses the MUK ID 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).

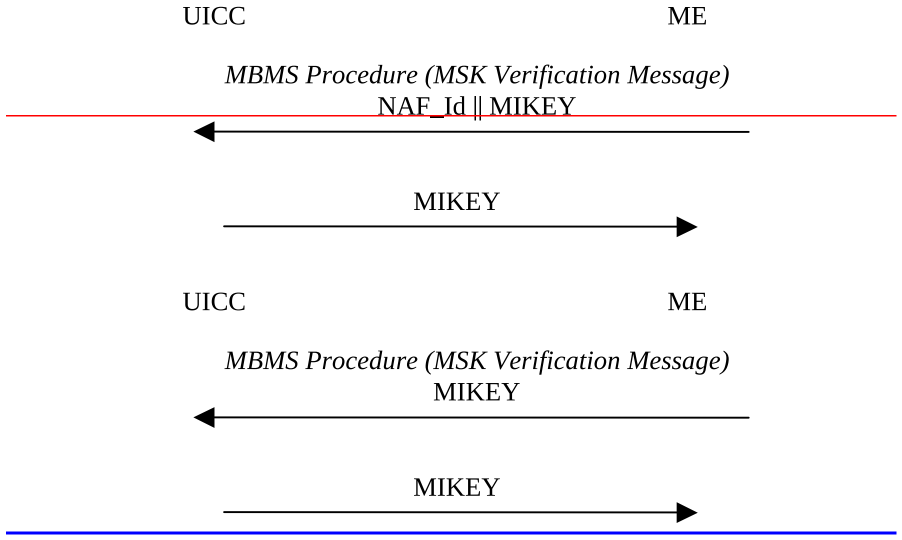

UICC
ME
MBMS Procedure (MSK Verification Message)
~~NAF_Id || MIKEY~~
MIKEY
UICC
ME
MBMS Procedure (MSK Verification Message)
MIKEY
MIKEY

**Figure D.2: MSK Verification Message**