3GPP TSG SA WG3 Security — S3#36 **S3-041011**

Shenzhen, China, November 23-26, 2004

Source: **Siemens**

Title: **Reliable MSK updating**

Document for: **Discussion and Decision**

Agenda Item: **MBMS**

1 Introduction

The Push solicited pull MIKEY message was defined in order to efficiently trigger the UE about a needed MSK-update. Three examples usecases are described within the TS 33.246. This contribution analyses the usecases and the specific push solicited pull procedure and proposes to enhance the reliability of the MSK delivery.

2 The use of MIKEY solicit-messages.

2.1 Analysis of the example usecases.

Three example usecases of MIKEY solicited-pull messages are included within the TS within section 6.3.2.2.4[1]

"*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.*"

1) For the first usecase it is doubtful if security is enhanced by using the solicited pull method for 'in-service authentication'. It is unclear if the whole duration of the MBMS-service is meant or only during the active transmission period of the MBMS service. But independent from this, the question can be posed what fraudulent case this mechanism would detect? An MBMS UE is allowed to go offline and therefore will not respond to the MIKEY solicit-pull message. An MBMS UE will be authenticated anyhow each time when a ptp http procedure between the UE and the BM-SC is executed. Using the MIKEY solicited-pull method for triggering an authentication run is considered a waste of network resources; hence it is proposed to remove this first usecase from the list of examples (see proposed CR).

2) For the third usecase in order to re-key all UEs, the BM-SC will need to send individual MIKEY messages to all active reachable UEs which belong to that service. It may be more efficient to use a broadcast channel announcement channel for this purpose, but that currently does not contain any means to indicate MSK ID (See NOTE section 6.3.2.2.2 Initiation of Key management) and has the disadvantage that the originator of the announcement message cannot be authenticated. So here no changes are proposed and the usecase is considered valid.

3) The second usecase has an unclear purpose (I.e. when the MUK has expired) because the MIKEY message needs a MUK for the MAC since the MIKEY message needs to be integrity protected. Specification TS 33.246 does not contain any specification on MUK/MRK-lifetime. The lack of MUK-lifetime specification in TS 33.246 could be interpreted in different ways. The most obvious interpretation is to refer to TS 33.220 specified Ks_xx_NAF key lifetime concept and to handle this very strictly. In the next section it will be shown that this may lead to an inefficient MSK handling.

[1] CR21-S3-040889

2.2 MUK-lifetime handling

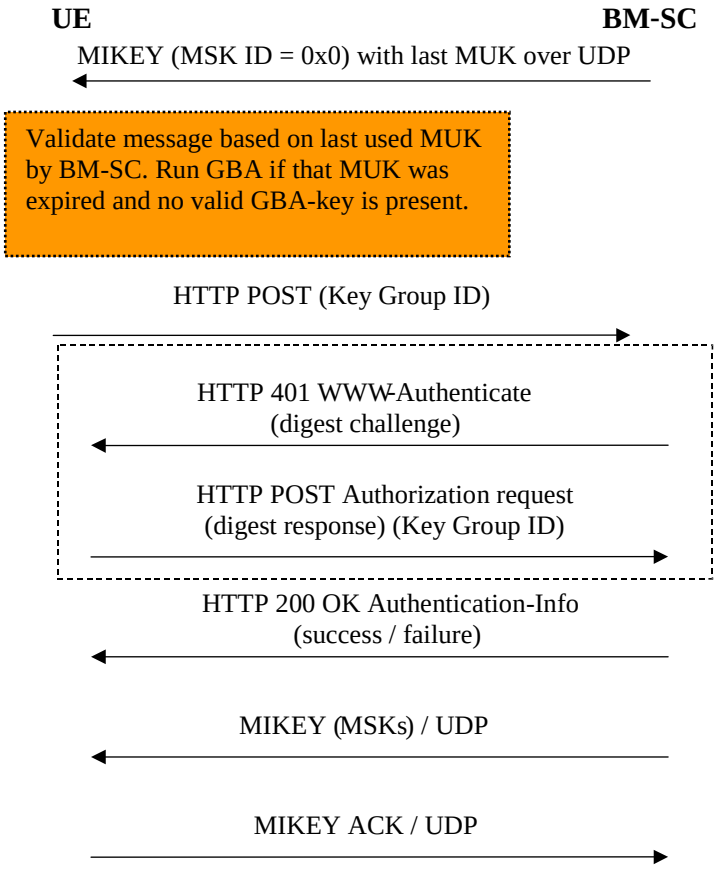
According to TS 33.220 a NAF has a means to trigger a GBA-bootstrapping by using a 'negotiation indication required' in the http response message. This method is useful for UE initiated Ua-services where the UE uses a non-expired GBA-key but the NAF policy requires an earlier NAF key refresh.

For MBMS that also contains NAF (i.e. BM-SC) initiated ptp-messages (e.g. like the solicited pull), it may happen that there is no valid MUK anymore at the BM-SC, or the MUK is considered expired at the moment that the message is processed at the UE. A UE **behaving strictly** on the lifetime shall reject all MIKEY messages which uses a MUK with expired lifetime. Such a MIKEY Message will therefore be rejected in a similar way as if it is mall-formed or contains a wrong MAC. So whenever this happens, the push-solicited pull procedure fails, and the UE will have to wait for a new MSK triggered by a mismatch. ***So with a strict MSK lifetime interpretation at the UE, the push solicited pull mechanism will fail in the circumstances that are described above***. The negative effect is that the MSK update will be delayed until there is a UE-initiated ptp connection to the BM-SC (e.g. due to ptp repair necessity or MSK key mismatch detection at the UE). It should be avoided that the latter of the two happens for many UEs at the same time as it might lead to a burst of MSK key requests to the BM-SC.

A design goal is to have reliable MBMS services, without much key management overhead i.e. the UE needs to have the MSK well in time before it is used for MTK transfer. Otherwise the UE could miss the actual start of a session if the MSK fetching takes too long.

One solution it to require that MTK-updates are send to the UEs well in time (Δ) before the MTK is being taken into use. This might require that the MBMS-bearers (including a different port for the MTK-updates) have to be set-up some time Δ before the actual MBMS session starts. Such an MTK-update message could even include a dummy MTK-value or an MTK-value that would be skipped from using. This limits the MTK-exposure time to a minimum. A UE that cannot validate the correctness of the MIKEY MTK message (because the MSK-ID is unknown and that the MTK-ID is allowed) will have no assurance of the integrity of the message. A DoS attack is therefore possible (injecting messages with unknown MSK-ID on the MBMS bearers), but note that this vulnerability is applicably to the MSK-ID mismatch UE behaviour in general. This seems to be configuration issue and therefore needs no specification modifications.

Another solution would be allowing the use of an expired MUK (i.e. beyond the BSF indicated key lifetime) for the Push solicited pull message exclusively. In order to ensure that the MSK-payload is protected with a fresh MUK, the BM-SC shall use a 'negotiation indication required' in the http response message of the in clause 6.3.2.2.1 specified Basic MSK retrieval procedure (S3-040889) if the UE did not use a fresh MUK. The UE should use a valid GBA-Key for the first http-request following the solicited pull MIKEY message that uses an expired MUK Key. The BM-SC and the UE therefore always need to store the last negotiated MUK (even if it is expired) in order to serve as a means to authenticate the push solicited pull MIKEY message. Performing no authentication on the push solicited pull MIKEY message would make it a tool for a hacker to perform a DoS attack to the BM-SC. The solution that was described in the previous clause seems to complement the 'expired MUK' solution in that it serves those MBMS-users which could not be reached by the BM-SC or where the push solicited pull MIKEY message over UDP was lost.



3 Conclusions

This contribution has shown that a strict MUK–life handling at the UE will create additional key management messages which could be avoided. It is proposed to allow the reuse of a MUK beyond the indicated ks_xx_NAF key lifetime settings only for the purpose of sending a push solicited pull MIKEY message.

It is proposed to approve the change requests that are available as attachment to this contribution.

4 Appendix (Section 6.3.2.2.4)

This appendix contains the content of TS 33.246 section 6.3.2.2.4 i.e. after approval of CR021Rev2 (S3-040889 from SA3#35)

6.3.2.2.4 BM-SC solicited pull

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

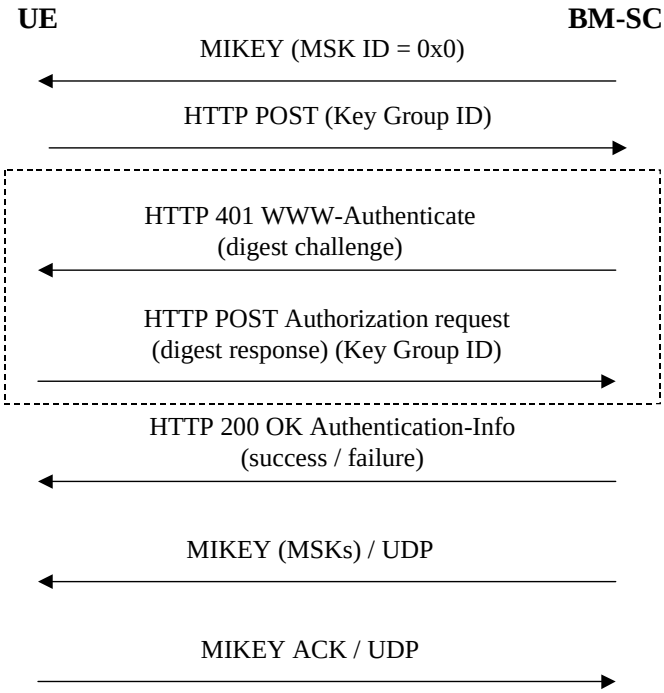


Figure 6.3: BM-SC solicited pull

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

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

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

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

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

Tdoc ⌘Att1_S3-041011

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **027** ⌘**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 [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	MUK lifetime handling with push solicited pull procedure
Source:	⌘	Siemens
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:

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:	⌘	- Allow the use of a MUK beyond the indicated ks_xx_NAF key lifetime settings only for the purpose of sending a push solicited pull MIKEY message. - Remove the usecase 'during service authentication' while this does not enhance the security.
Summary of change:	⌘	Clarify the usecases and the MUK lifetime handling for the push solicited pull procedure.
Consequences if not approved:	⌘	A strict MUK key life handling at the UE will create additional key management messages which could be avoided.
Clauses affected:	⌘	6.1 and 6.3.2.3.2

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

Other comments:	⌘	This CR shows the changes when implemented on 33.246v600 as a standalone CR. It is proposed to approve revisions of accepted CRs of the Malta meeting i.e. S3-040863 (att2) and S3-040889 (att3) Note that S3-040889 was based on 33.246v200 and needs to be upgraded.

===== BEGIN 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.

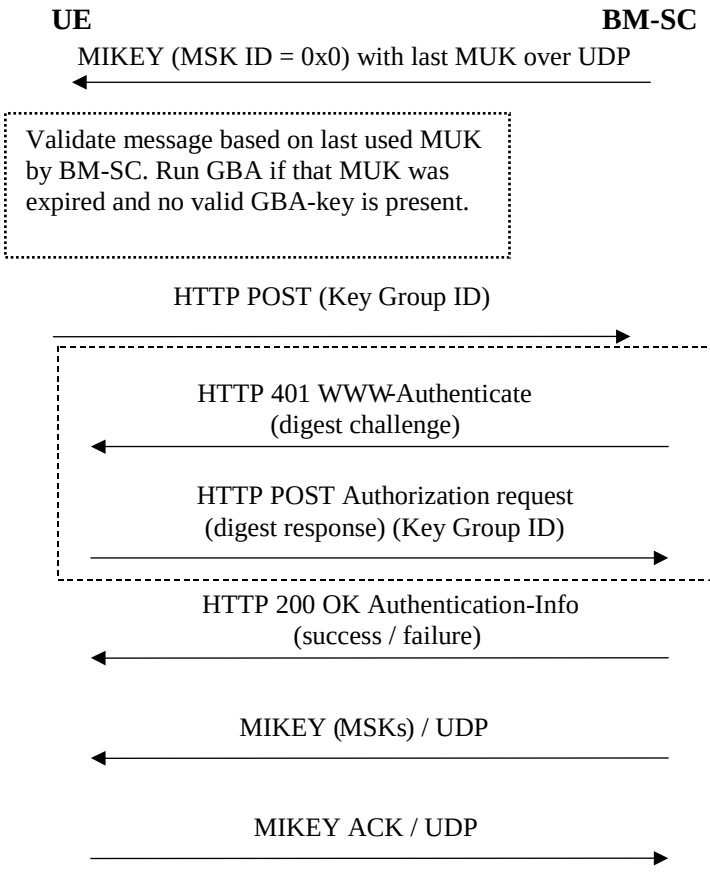
For ME based key management, the ME shall store the last successfully used MUK in non-volatile memory in order to be able to authenticate the first MIKEY message of a push solicited pull procedure (cf. clause 6.3.2.3.2).

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

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

6.3.2.3.2 Push 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 MSKs. An example of such situation is when the BM-SC wants to trigger a UE that is needs to update the MSK~~the UE to authenticate itself during the service or when the MUK has expired~~.


UE
BM-SC
MIKEY (MSK ID = 0x0) with last MUK over UDP
Validate message based on last used MUK by BM-SC. Run GBA if that MUK was expired and no valid GBA-key is present.
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

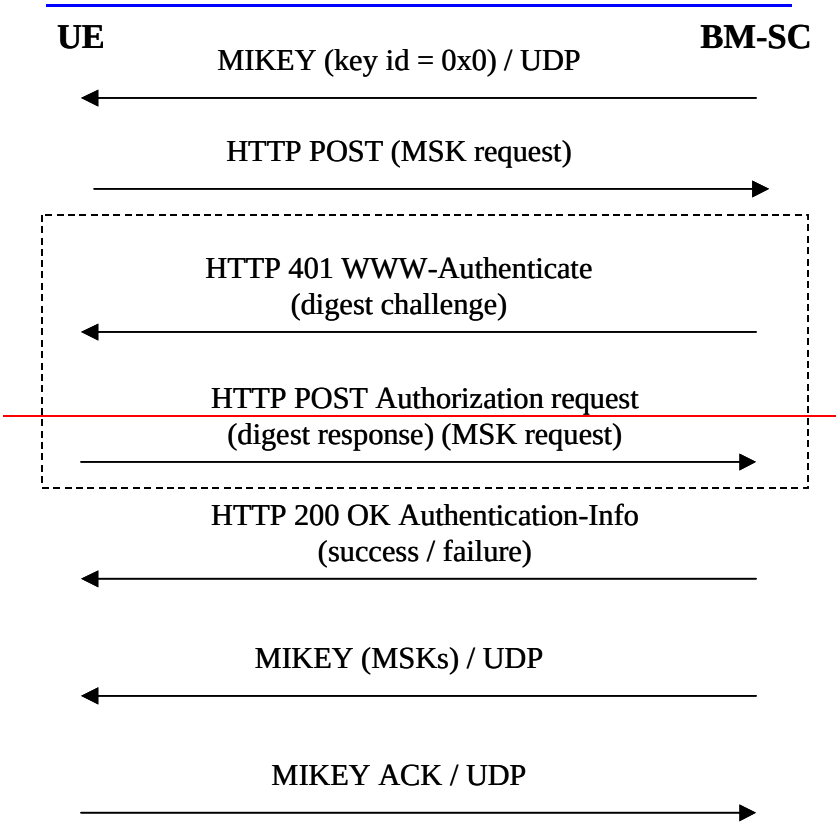

UE
BM-SC
MIKEY (key id = 0x0) / UDP
HTTP POST (MSK request)
HTTP 401 WWW-Authenticate (digest challenge)
HTTP POST Authorization request (digest response) (MSK request)
HTTP 200 OK Authentication-Info (success / failure)
MIKEY (MSKs) / UDP
MIKEY ACK / UDP

Figure 6.3: Push 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 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.

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 that MUK within the first MIKEY message of a push solicited pull procedure.

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.

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

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

Tdoc ⌘ Att2_S3-041011

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **001** ⌘ **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 ☐

Title:	⌘	Deletion of MBMS keys stored in the ME
Source:	⌘	Siemens
Work item code:	⌘	MBMS
Date:	⌘	09/11/2004
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 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 shall store the last successfully used MUK in non-volatile memory in order to be able to authenticate the first MIKEY message of a push solicited pull procedur
Consequences if not approved:	⌘	Insecure ME Based key management if MBMS keys are not deleted at UICC change.

Clauses affected:	⌘	6.1
Other specs affected:	⌘	Y / N ☐ / X Other core specifications ⌘ ☐ / X Test specifications ☐ / X O&M Specifications
Other comments:	⌘	Changes with respect to revision 2 have yellow colour.

***** 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 shall store the last successfully used MUK 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 user will need to request MSK to the BM-SC and may need to run GBA to reconvene an MBMS session.

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

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

Tdoc ⌘Att3_S3-041011

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **021** ⌘ **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:	⌘	Clarification of MSK key management
Source:	⌘	Siemens
Work item code:	⌘	MBMS
Date:	⌘	16/11/2004
Category:	⌘	**C**
Release:	⌘	Rel-6

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

Use one of the following releases:

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

Reason for change:	⌘	Initiation of key management is not specified. The details of MSK request from UE to the BM-SC are unclear. The details of MIKEY solicit message from the BM-SC are unclear. The structure of the MSK procedure sections are enhanced. The split to pull and push procedures is seen to be more clear and enable smoother update of the TS in the future, if for example new triggers are introduced for pulling the MSK from the BM-SC like initiation of key management
Summary of change:	⌘	Initiation of key management is specified. Required Security parameters in Service Annoucement are specified. It is specified that the UE shall request for the Key Group ID(s) from the BM-SC. MSK ID(s) are not needed in the request since BM-SC will send the current valid MSK for each Key Group ID. BM-SC should solicit the UE to contact the BM-SC by setting the MSK ID to 0x0 in the MIKEY MSK message. The message will not carry any MSK. 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, 6.3.2.3
Other specs affected:	⌘	Y N ☐ ☒ Other core specifications ⌘ ☐ ☒ Test specifications ☐ ☒ O&M Specifications
Other comments:	⌘	The changes with respect to revision 2 of the CR have yellow colour

2 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.3.2 MSK procedures

6.3.2.1 MSK identification

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

where

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

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

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

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

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

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

6.3.2.2.1 Basic MSK retrieval procedure

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

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

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

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

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

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

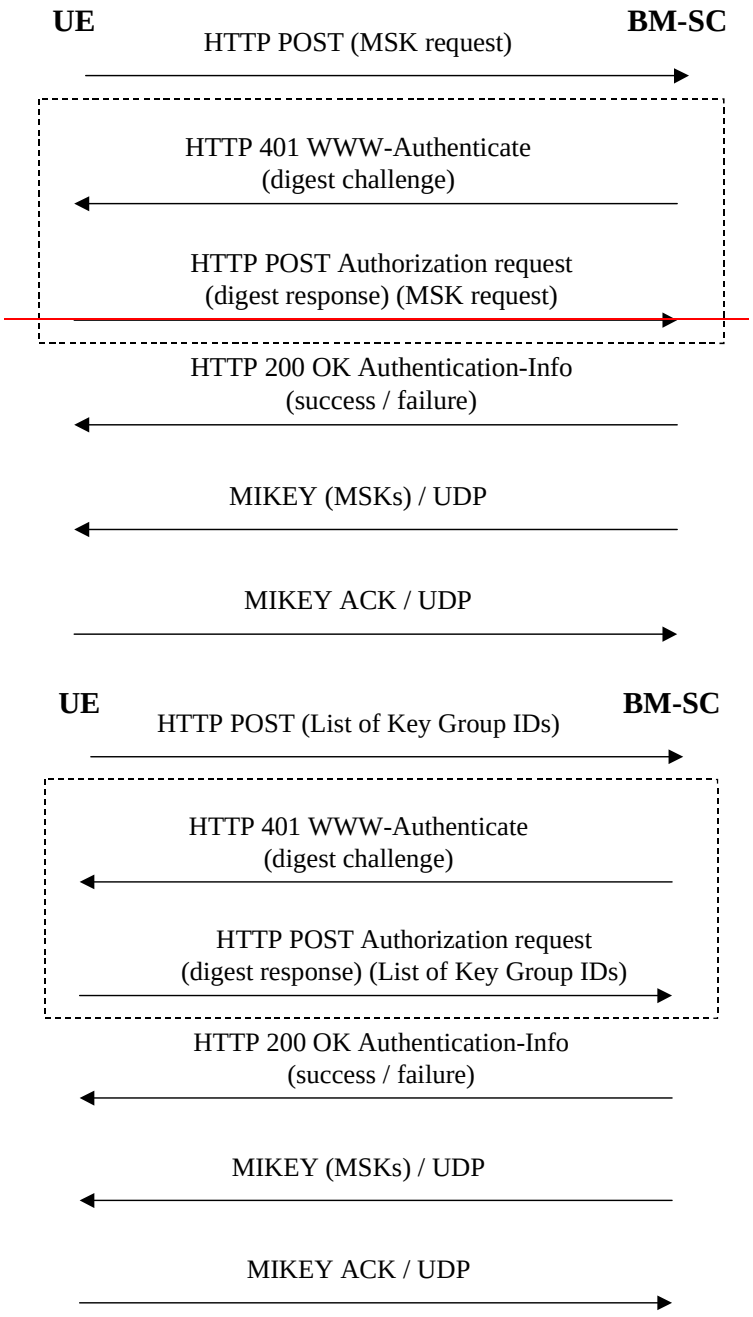


Figure 6.1: ~~UE initiated MSK delivery~~Basic MSK retrieval procedure

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

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

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

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

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

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

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

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

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

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

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

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

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

6.3.2.2.2 Initiation of key management

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

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

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

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

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

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

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

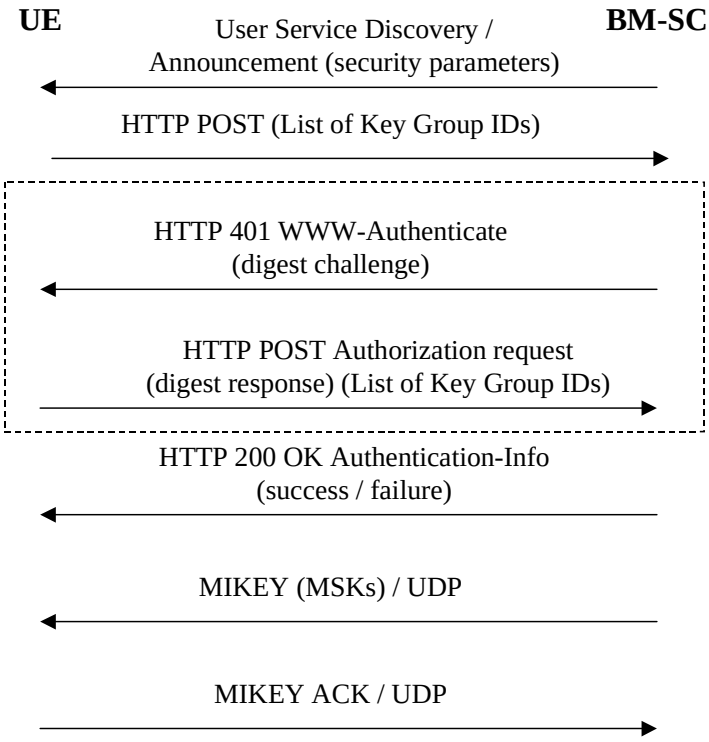


Figure 6.x: MSK retrieval procedure

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

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

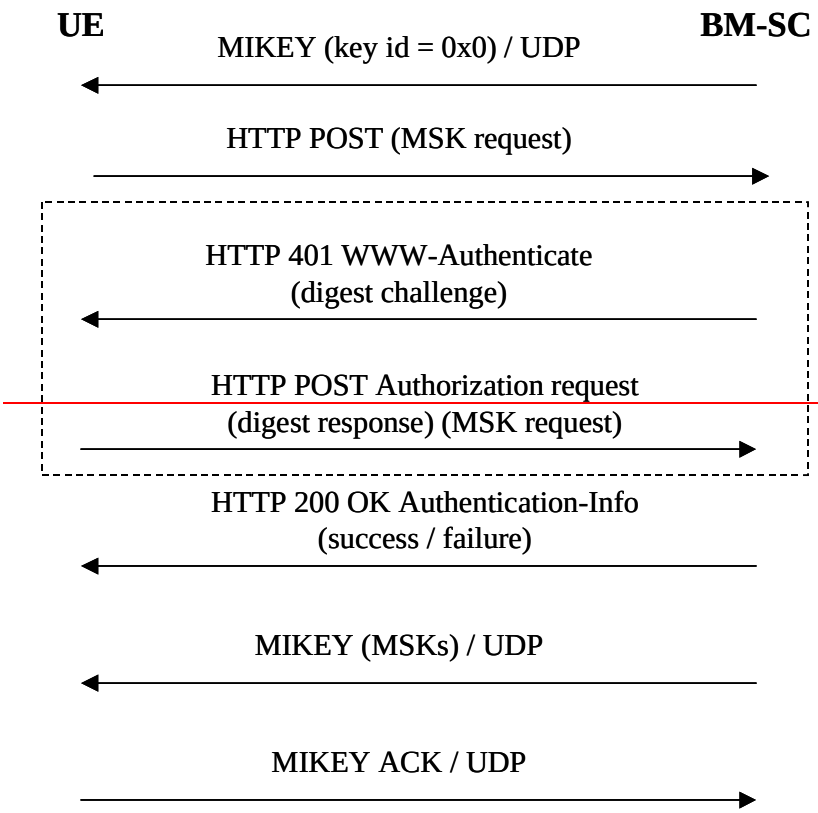
The rest of the procedure is the same as in 6.3.2.3.1.

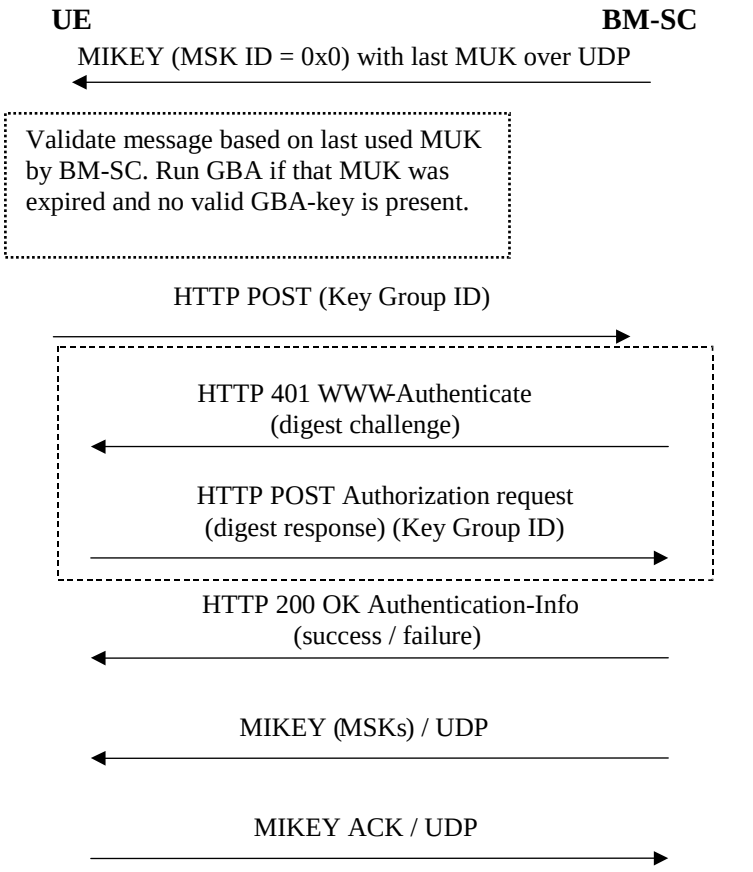
6.3.2.2.3 Missed key update procedure

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

6.3.2.2.4 BM-SC solicited pull

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


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



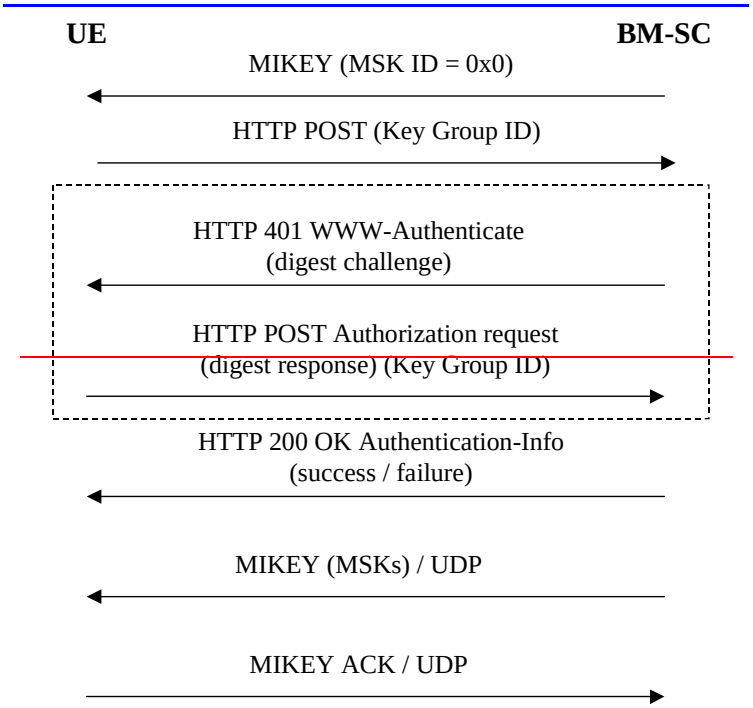


Figure 6.3: BM-SC solicited pull

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 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 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.

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.

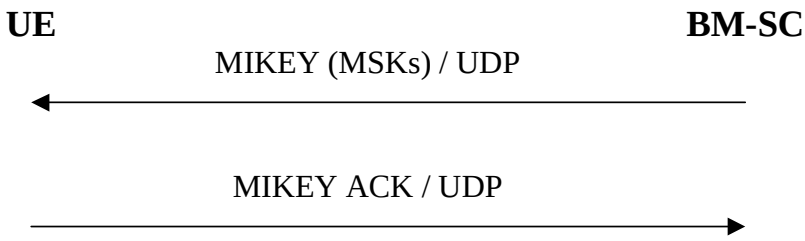


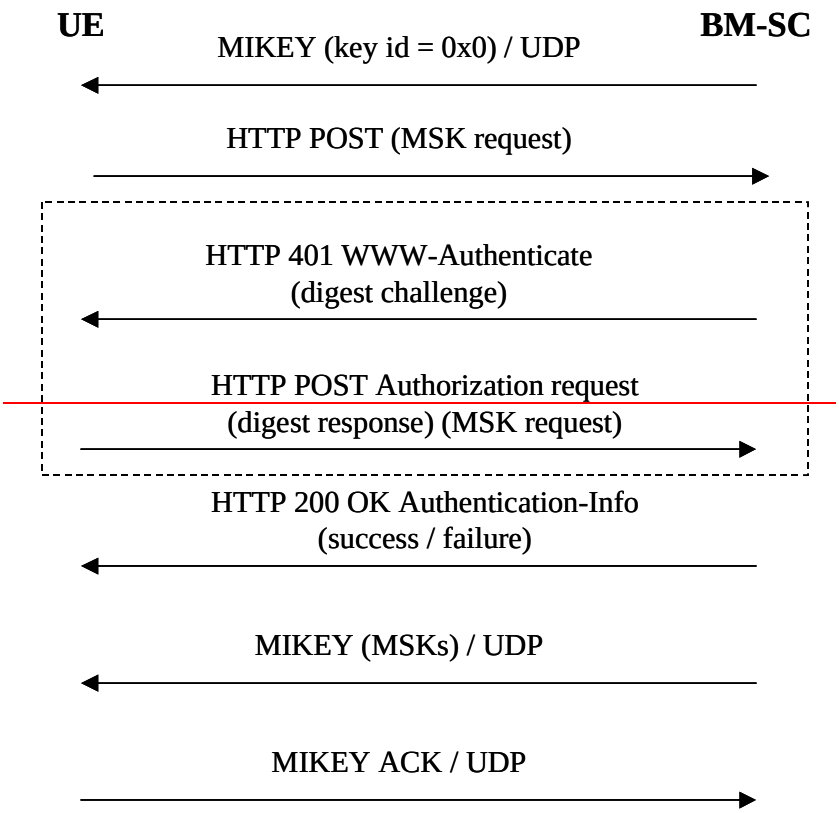
Figure 6.2: Pushing the MSKs to the UE

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.~~