

CHANGE REQUEST

⌘ **33.246 CR 021** ⌘ rev **7** ⌘ 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:	⌘ Thursday MBMS drafting group		
Work item code:	⌘ MBMS	Date:	⌘ 25/11/2004
Category:	⌘ C	Release:	⌘ Rel-6
	Use <u>one</u> 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)		Use <u>one</u> 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)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		

Reason for change:	⌘ Initiation of key management is not specified. Required Security parameters in Service Announcement are not specified. The details of MSK request from UE to the BM-SC are unclear. The details of MIKEY solicit message from the BM-SC are unclear. The structure of the MSK procedure sections are enhanced. The split to pull and push procedures is seen to be more clear and enable smoother update of the TS in the future.
Summary of change:	⌘ Initiation of key management is specified. Required Security parameters in Service Announcement are specified. The details of UE requesting for MSKs is specified. The details of BM-SC solicited pull are specified. The BM-SC shall be allowed to use a MUK beyond the ks_xx_NAF lifetime for the purpose of MSK update trigger.
Consequences if not approved:	⌘ Initiation and details of MBMS key management messages remain unspecified.

Clauses affected:	⌘ 2, 6.3.2.2, 6.3.2.2.1 (new), 6.3.2.2.2 (new), 6.3.2.2.3 (new), 6.3.2.2.4 (new), 6.3.2.3, 6.3.2.3.2 (void)										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications ⌘ Test specifications ⌘ O&M Specifications ⌘	
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
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 *****

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

6.3.2.2.1 Basic MSK retrieval procedure

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

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

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

~~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

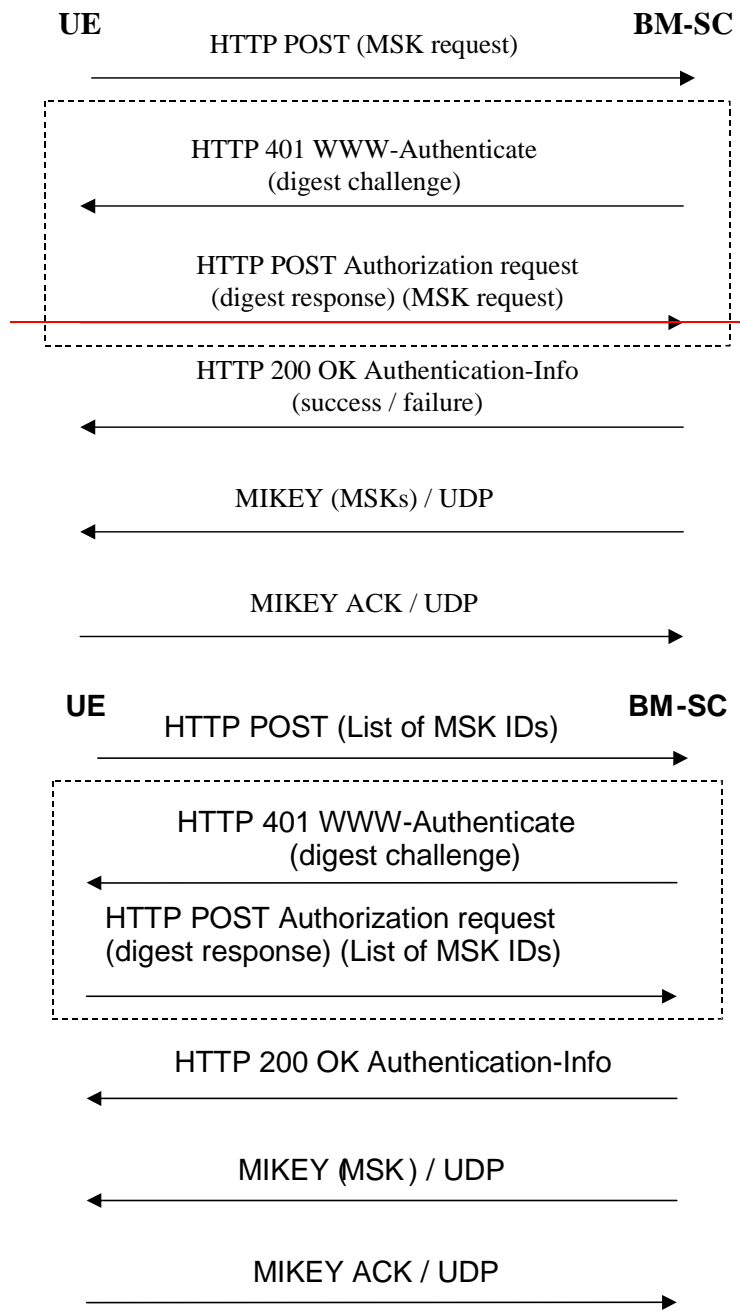


Figure 6.x4: ~~UE initiated MSK delivery~~ Basic MSK retrieval procedure

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

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

- key identification information: a list of MSK IDs-

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

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.~~

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

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 messages ~~procedures~~ over UDP transporting the requested MSKs to the UE.

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

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

6.3.2.2.2 Initiation of key management

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

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

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

- Fully qualified domain name of the key management server (i.e. the BM-SC). This for the UE to know to which IP address to send the MSK request
- Confidentiality protection: on / off
- Integrity protection: on / off
- UICC key management required: yes/ no
- Identifiers of the MSKs needed for the User Service

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

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

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.

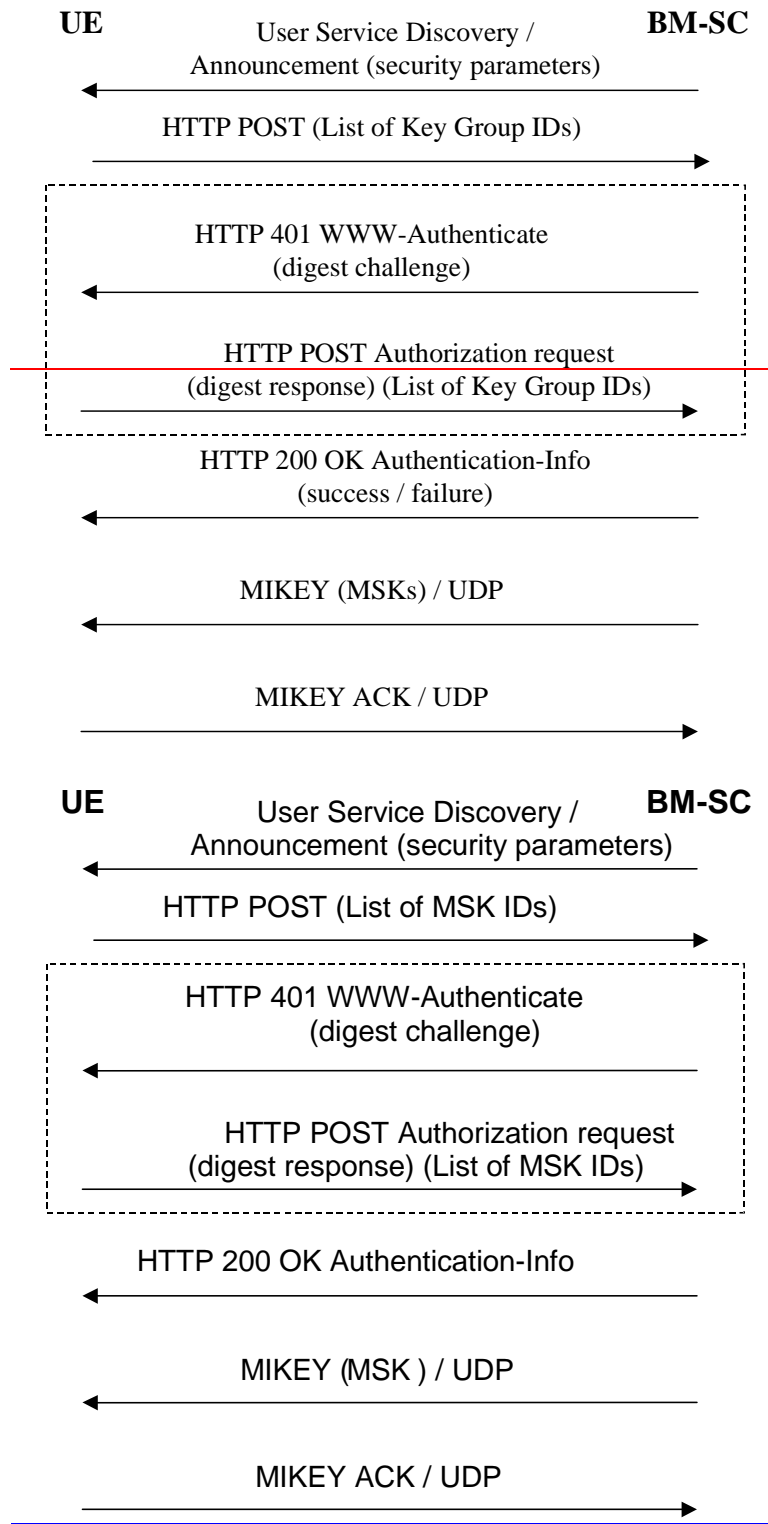


Figure 6.x: MSK retrieval procedure

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

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

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

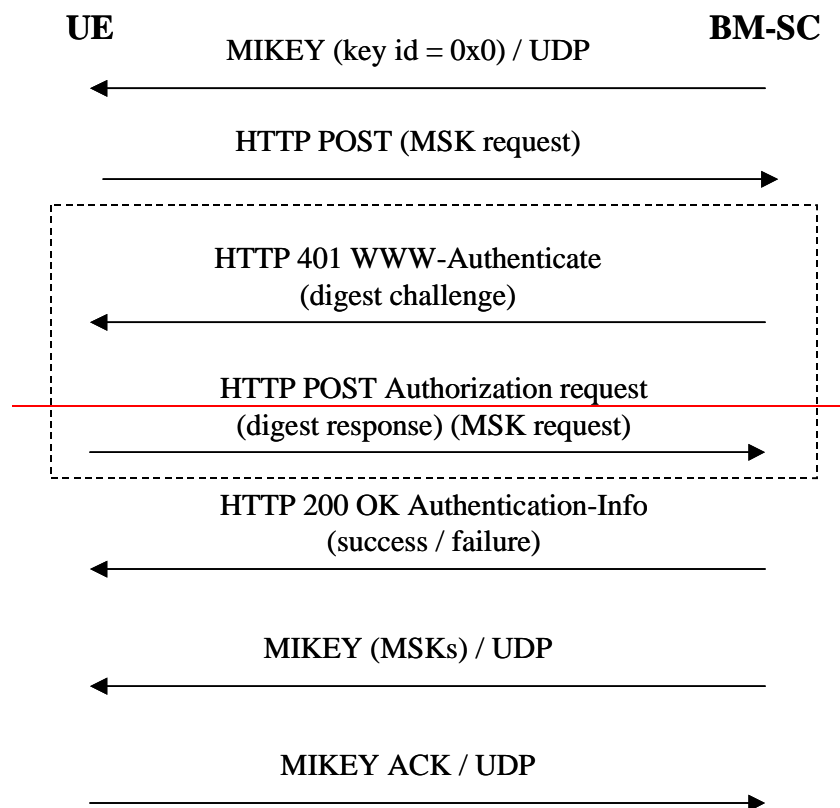
[The rest of the procedure is the same as in 6.3.2.3.1.](#)

[6.3.2.2.3 Missed key update procedure](#)

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

[6.3.2.2.4 BM-SC solicited pull](#)

[While the push is the regular way of updating the MSK to the UE, there may be situations where the BM-SC solicits the UE to contact the BM-SC and request for new MSK. Examples of such situations are when the BM-SC wants the UE to trigger a UE that it needs to update the MSK.](#)



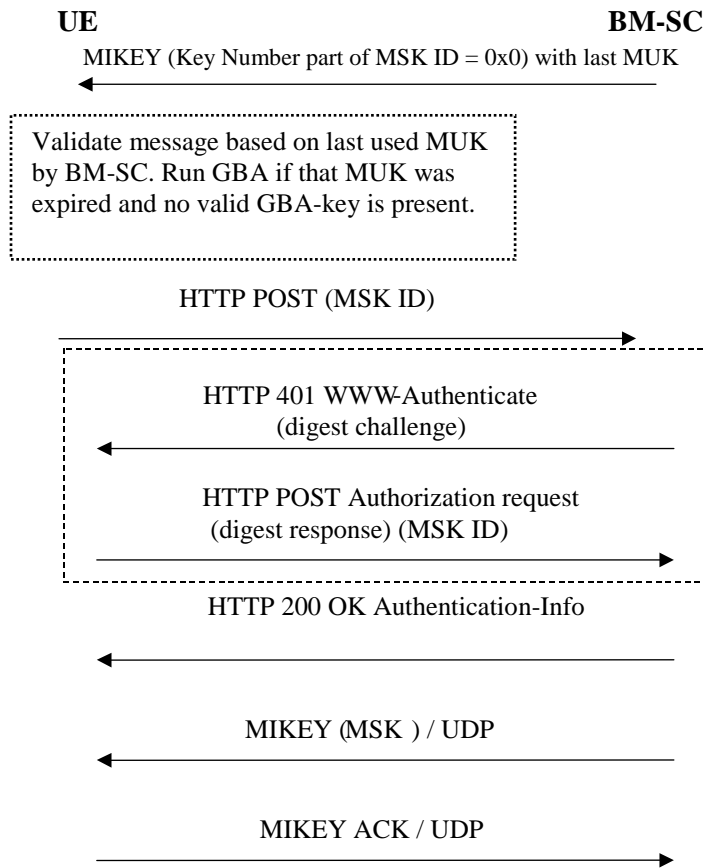


Figure 6.x: BM-SC solicited pull

The BM-SC sends a MIKEY message over UDP to the UE. The MIKEY message shall be protected by the most recent MUK known by the BM-SC. The Key Number part of the MSK ID in the extension payload of the MIKEY message shall be set to 0x0 to indicate that the UE should request for current MSK from the BM-SC.

NOTE: A MUK may be used by the BM-SC beyond the GBA key lifetime of the corresponding Ks_{xx} NAF for the purpose of using the MUK within the first MIKEY message of a push solicited pull procedure.

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

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

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

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

6.3.2.3.1 Pushing the MSKs to the UE

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

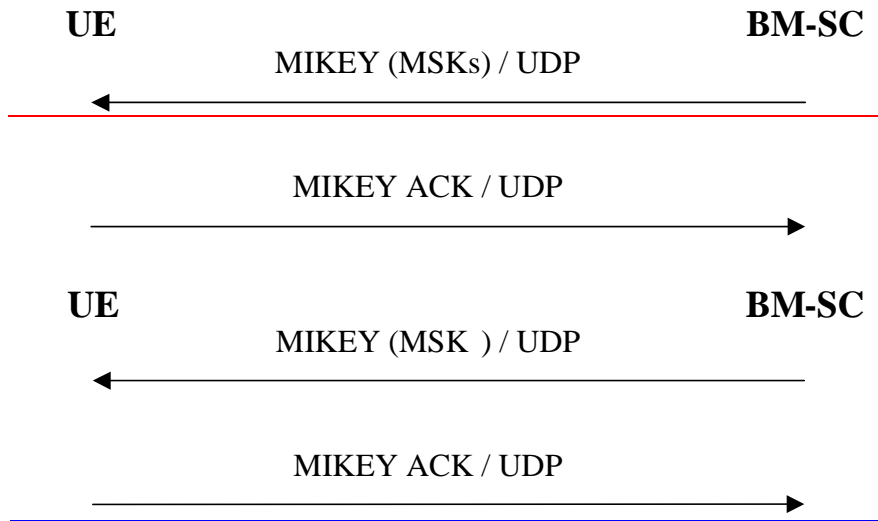


Figure 6.2: Pushing the MSKs to the UE

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

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

6.3.2.3.2 ~~Push solicited pull~~ Void

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

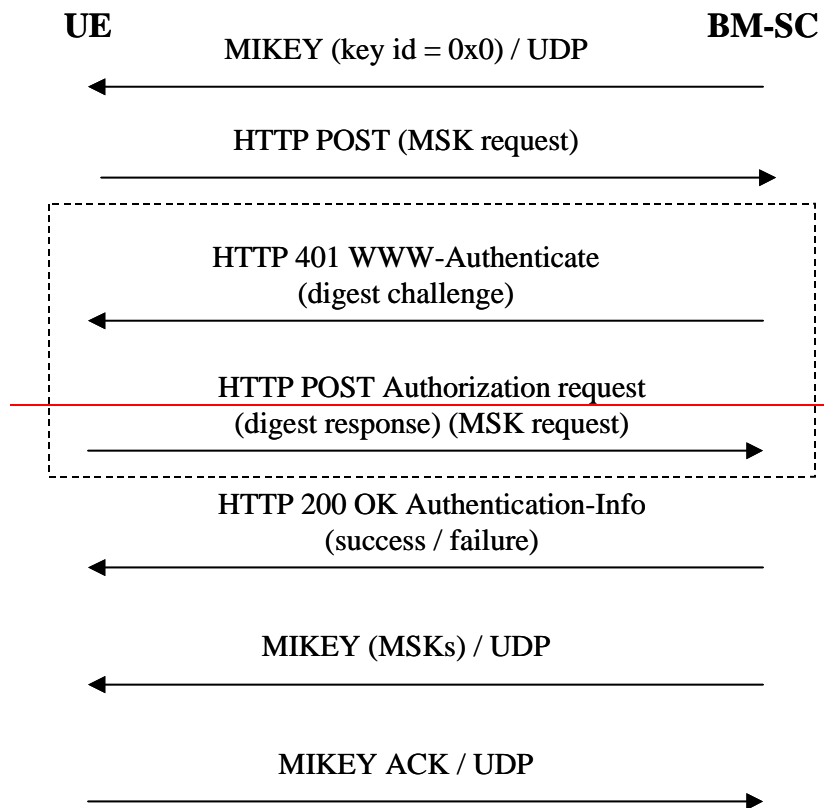


Figure 6.3: Push-solicited pull

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

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

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