3GPP TSG-SA WG3 Meeting S3#37
Sophia, France, 21-25 February, 2005

Tdoc ⌘S3-050084

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **047** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	Clarification of MSK and MTK procedures
Source:	⌘	Ericsson
Work item code:	⌘	MBMS
Date:	⌘	14/2/2005
Category:	⌘	**C**
Release:	⌘	Rel-6

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

Use one of the following releases:
Ph2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*
Rel-7 *(Release 7)*

Reason for change:	⌘	It is unclear when the key management is initiated. Also, current description of MSK procedures is misleading since it gives the impression that MSK is delivered within MSK retrieval procedure although this procedure is used to request the MSK and MSK is then delivered with its own procedure. In addition the reliability mechanisms of MTK deliveries are underspecified.
Summary of change:	⌘	The following issues are clarified: • key management is initiated when an MSK is requested for the first time • MSK procedures are clarified to include MSK request and MSK delivery procedure • it is clarified that key management is not initiated if both confidentiality and integrity protection are indicated to be 'off' in the service announcement • reliability of MTK messages in streaming is based on repetition and on FLUTE features in download
Consequences if not approved:	⌘	Unclear specification and possible interoperability problems.

Clauses affected:	⌘	6.3.1, 6.3.2.2, 6.3.2.2.1, 6.3.2.2.2, 6.3.2.2.2, 6.3.2.2.4, 6.3.2.3, 6.3.2.3.1, 6.3.3.2, 6.3.3.2.1, 6.3.3.2.2

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

Other comments: ⌘

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

6.3.1 General

In order to protect an MBMS User service, it is necessary to ~~transfer~~ deliver both MSKs and MTKs from the BM-SC to the UE.

MSK procedures are further divided to MSK request procedures, described in clause 6.3.2.2, and MSK delivery procedure, described in clause 6.3.2.3. MSK procedures use a point-to-point bearer. MSK procedures are similar for both streaming and download services. ~~Clause 6.3.2 describes the possible procedures for transferring MSKs, while clause 6.3.3 deals with the transfer of MTKs.~~

MTK delivery procedures use the MBMS bearer. MTK delivery procedures are different for streaming and download services and they are described in clause 6.3.3.

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

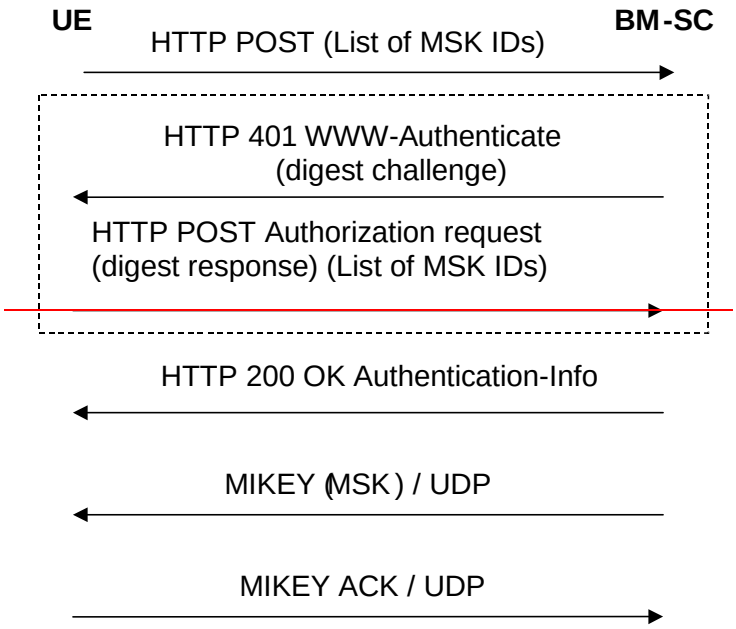
6.3.2.2 MSK ~~retrieval~~ request procedures

6.3.2.2.1 Basic MSK ~~retrieval~~ request procedure

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

The basic MSK ~~retrieval~~ request procedure is a part of different other procedures, e.g.:

- initiation of key management when the UE has joined the MBMS user service;
- ~~retrieval~~ request of MSK(s) when the UE has missed a key update procedure e.g. due to being out of coverage.
- BM-SC solicited pull.



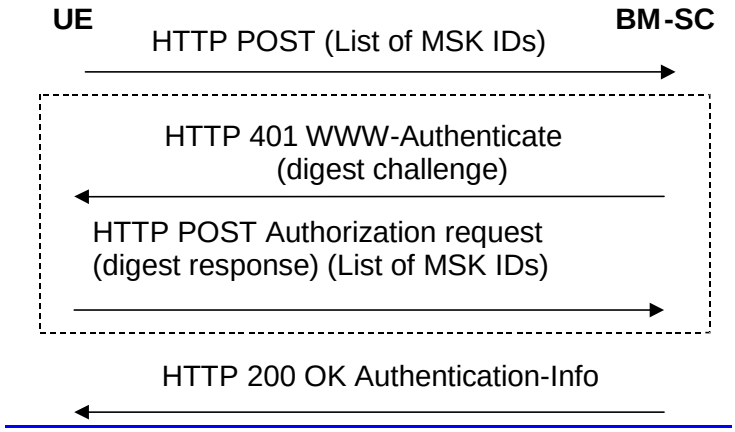


Figure 6.1: Basic MSK ~~retrieval~~ request procedure

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

The UE requests for the MSKs using ~~WITH~~ the HTTP POST message. The following information is included in 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 clause 6.2.1 and verifies that the subscriber is authorized to receive the MSKs for this service.

NOTE: The BM-SC may not need to challenge the UE (dashed box in Figure 6.1), if the UE has used WWW Authorization request headers in the first message in Figure 6.1 and BM-SC is able to authenticate the UE.

If the authentication is successful then the BM-SC sends a HTTP 200 OK message with Authentication-Info header. If the authentication fails 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 HTTP procedure above resulted to success, the BM-SC initiates MSK delivery procedure as specified in clause 6.3.2.3.

NOTE: The time between the MSK request procedure and MSK delivery procedure may vary, i.e. the UE should not expect the MSK delivery procedures to start immediately. ~~MIKEY message 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 as specified in clause 6.3.2.2.1.

When the BM-SC receives the first MSK request for a specific Key Group (indicated in the Key Group part of the MSK ID), the BM-SC shall consider this as initiation of key management for that Key Group for the requesting UE.

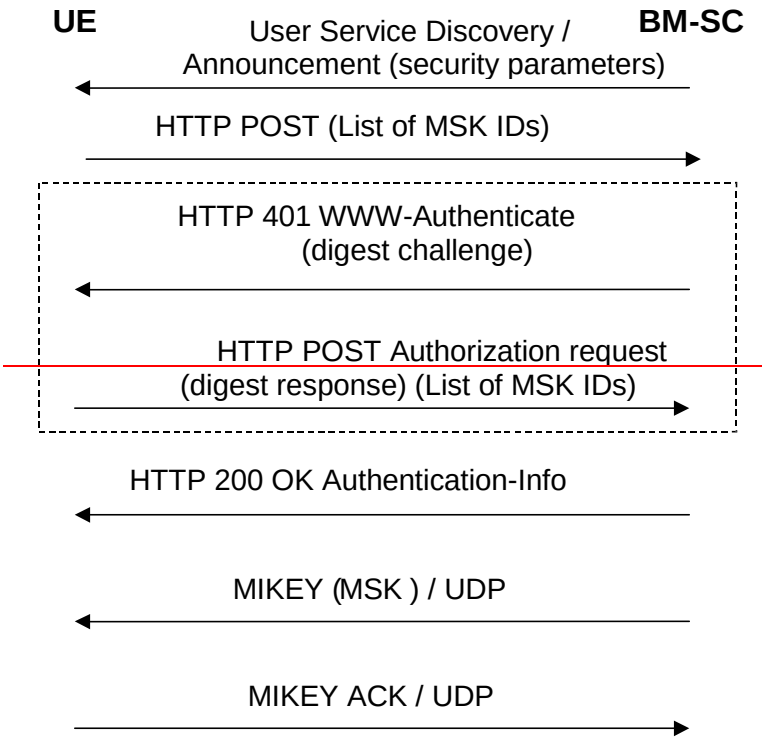
NOTE: The User Service Discovery / Announcement procedures are specified in TS 26.346 [13]. It is out of the scope of the present specification how the UE receives the User Service information and how the User Service is triggered in the UE.

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 is 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 in Service Announcement 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 6.2a: MSK retrieval procedure**~~

In case both confidentiality and integrity protection are indicated 'off' for this service description, the UE should not initiate key management.

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 clause 6.2.1 of this specification.~~

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

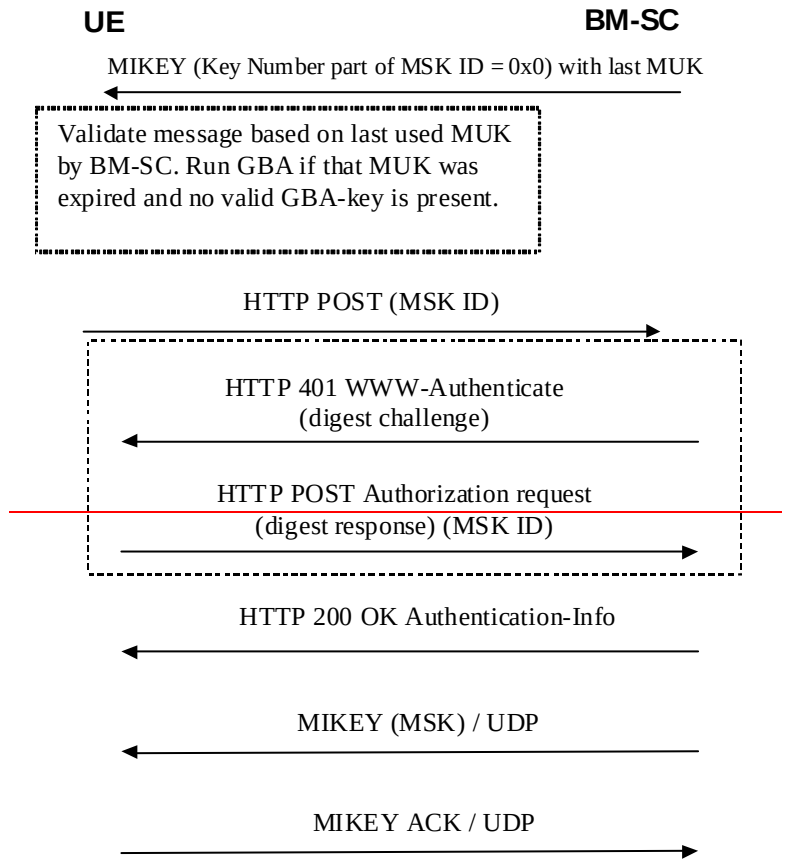
~~The rest of the procedure is the same as in clause 6.3.2.3.1.~~

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 clause 6.3.2.2~~3~~.1.

6.3.2.2.4 BM-SC solicited pull

While the push is the regular way of updating the MSK to the UE, there may be situations where the BM-SC solicits the UE to contact the BM-SC and request for new MSK. An example of such a situation is when the BM-SC wants the UE to trigger a UE that it needs to update the MSK.



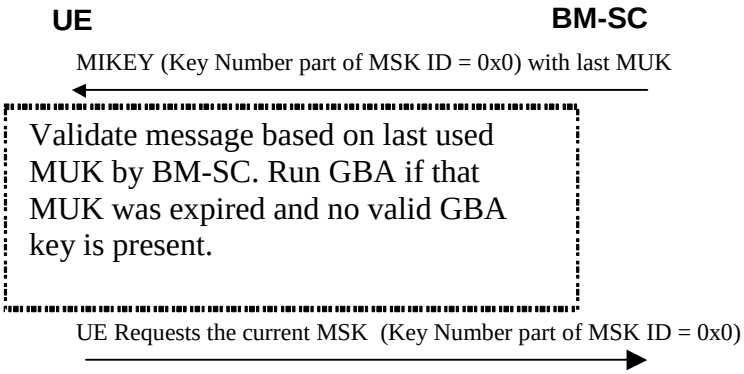


Figure 6.2b: BM-SC solicited pull

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 1: 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 2: 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 as specified in clause 6.3.2.2.1. ~~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 TS 33.220 [6].~~

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

6.3.2.3 MSK ~~push~~ delivery procedures

6.3.2.3.1 Pushing the MSK~~s~~ 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. This procedure can be initiated after the UE has requested for MSK(s) as described in clause 6.3.2.2.

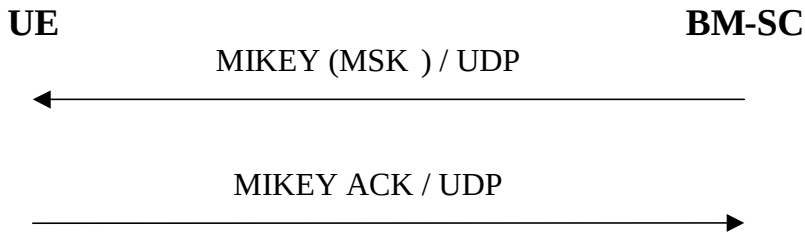


Figure 6.3: Pushing the MSKs to the UE

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

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

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

6.3.3.2 MTK update procedure

The MTK is delivered to the UE using MIKEY over UDP, ~~as in 6.3.2.3.1~~ but the MIKEY ACK is not used.

6.3.3.2.1 MTK delivery in download

In the download case the MIKEY message carrying the MTK shall be delivered over the same FLUTE stream as the object to be downloaded to the UE (see TS 26.346 [13]). This means that the message is specified as a separate object in the FLUTE File Delivery Table (FDT), having its own identifier. This means the MTK delivery inherits the reliability features of FLUTE. The mime-type of the object carrying the MIKEY message shall be the IANA-registered type for MIKEY.

6.3.3.2.~~1~~2 MTK delivery in streaming

MIKEY messages transporting MTKs shall be sent using the same IP destination address as the RTP traffic. MIKEY messages shall be transported to UDP port number 2269 specified for MIKEY. Reliability of MTK delivery is reached by re-sending MTK messages periodically. In order to increase the possibility that UEs receive a new MTK in time, MTK messages may be sent before the RTP traffic changes over to a new MTK.

Editor's Note: The UDP port number needs to be specified for MIKEY.