3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040565

CR-Form-v7

CHANGE REQUEST

⌘	**33.246**	**CR**	**CRNum**	⌘ **rev**	**-**	⌘	Current version:	**1.2.1**	⌘

*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:	⌘	Push and pull key management for MBMS			
Source:	⌘	Ericsson			
Work item code:	⌘	MBMS	***Date:***	⌘	29/06/2004
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:	⌘	The key management procedures have not been specified.
Summary of change:	⌘	Push and pull key management cases are added to the TS 33.246.
Consequences if not approved:	⌘	

Clauses affected:	⌘	6.3				
		Y	N			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

6.3 Key update procedures

6.3.1 UE initiated MSK update procedure

~~Once~~ When a UE detects that it needs the MSK(s) for a specific MBMS User service~~has joined a multicast service~~, the UE should try to get the MSKs that will be used to 'protect' the data transmitted as part of this multicast service. Reasons for UE to retrieve the MSK(s) include e.g.:

- Retrieval of initial MSKs e.g. when the UE has joined the MBMS user service

Editor's note: The initial key request can 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 MSKs when the UE has missed a key update procedure e.g. due to being out of coverage

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.

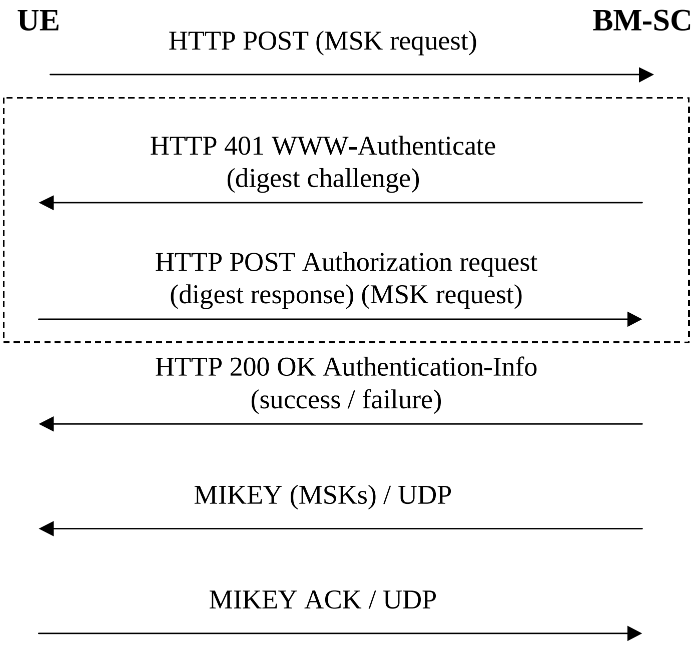

UE
BM-SC
HTTP POST (MSK request)
HTTP 401 WWW-Authenticate
(digest challenge)
HTTP POST Authorization request
(digest response) (MSK request)
HTTP 200 OK Authentication-Info
(success / failure)
MIKEY (MSKs) / UDP
MIKEY ACK / UDP

Figure x. UE initiated MSK delivery

The UE ~~tries~~ requests for ~~to get~~ the MSKs using the ~~second message in the below flow~~HTTP POST message []. The key identification information is included in the client payload of the HTTP message.~~–~~

The BM-SC 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.

If the key request procedure above resulted to success, the BM-SC sends MIKEY messages over UDP transporting the requested MSKs to the UE.

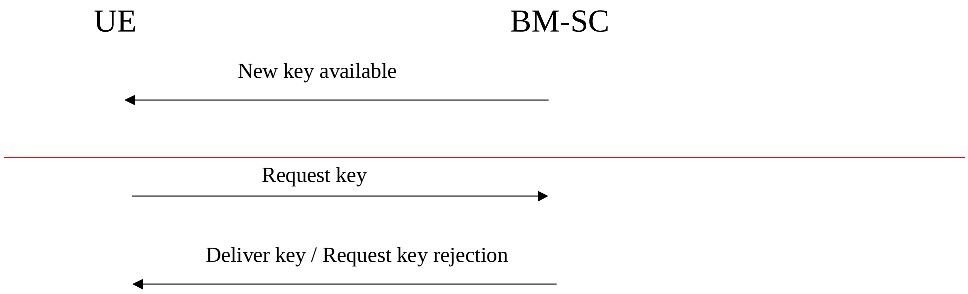
If requested by the BM-SC, the UE sends a MIKEY acknowledgement message to the BM-SC.

Editor's Note: The contents of the client payloads are FFS and may require input from TSG SA WG4.

6.3.2 BM-SC initiated MSK update procedures

6.3.2.1 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.



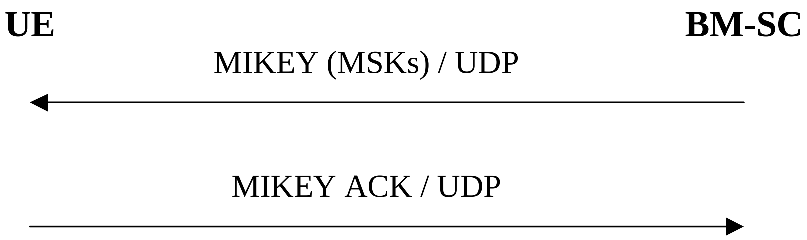


Figure x. Pushing the MSKs to the UE

When the BM-SC decides to 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.

6.3.2.1 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 the UE to authenticate itself during the service or when the MUK has expired.

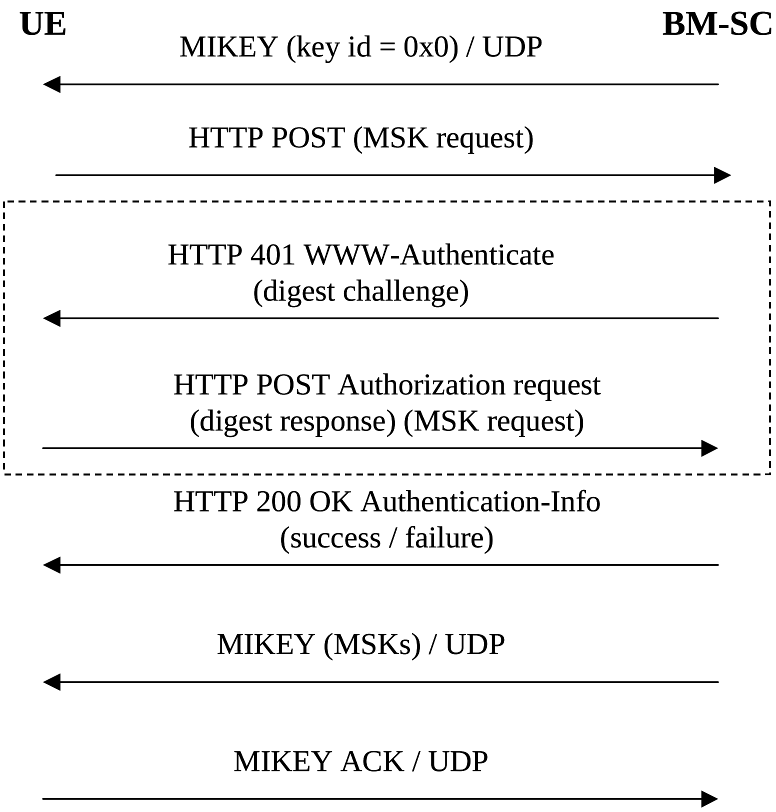

UE
BM-SC
MIKEY (key id = 0x0) / UDP
HTTP POST (MSK request)
HTTP 401 WWW-Authenticate
(digest challenge)
HTTP POST Authorization request
(digest response) (MSK request)
HTTP 200 OK Authentication-Info
(success / failure)
MIKEY (MSKs) / UDP
MIKEY ACK / UDP

Figure x. 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.

Editor's Note: The contents of the client payloads are FFS and may require input from TSG SA WG4.

.~~The first message is sent out by the BM-SC to indicate that new MSKs are available. It is an optional message in the flow. If it is sent to all UEs, then the BM-SC should provide the rules to the UE for subsequent request for the new MSK when a UE joins a multicast service, to avoid simultaneous requesting from all the UEs.~~

~~Editor's note: A possible method for achieving the above is for the BM-SC to allocates different "request delay time" to different UEs; such that when the UEs receive the new key available message, they shall send the request key message after the delay requested by the BM-SC. Alternatively it is possible to use the key lifetime methods suggested in S3-040059.~~

~~The second message is used to request an MSK. This is sent by the UE when it either receives the first message in the flow and does not have the new MSK, or has just joined a multicasts service and does not have an MSK for that service or has received some protected content and does not have the MSK that was used to protect the content. If the UE fails to get hold of the updated MSK or receive 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 service.~~

~~□After receiving the second message the BM-SC should send out the appropriate MSK to the UE protected by the relevant means, or reject the UE's key request with an indication of the cause. Upon successfully receiving the new MSK, the UE should store this key for later use.~~

~~Editor's note: MIKEY was chosen as the method for carrying keys. The use of MIKEY will be based on the proposal in S3-040258.~~

6.3.3 MTK update procedure

The MTK is delivered to the UE as in 6.3.2.1 but the MIKEY ACK is not used.