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

Tdoc ⌘S3-050091

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**052**	⌘**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⌘ ☒ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Introduction of BM-SC subfunctions		
Source:	⌘	Ericsson		
Work item code:	⌘	MBMS	***Date:*** ⌘	14/2/2005
Category:	⌘	**D**	***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 current specification lacks a proper security architecture overview and description of security sub-functions as defined in SA4 TS 26.346.
Summary of change:	⌘	New text to describe the MBMS security sub-functions. Clarification of Security architecture. The current CR implements the security related sub-functions as they are defined in version 1.5.0 of TS 26.346. It is proposed that the subfunctions are further discussed in the meeting and a new version of the CR can be produced in case adjustments are needed.
Consequences if not approved:	⌘	The specification will not be aligned with SA4 TS 26.346.

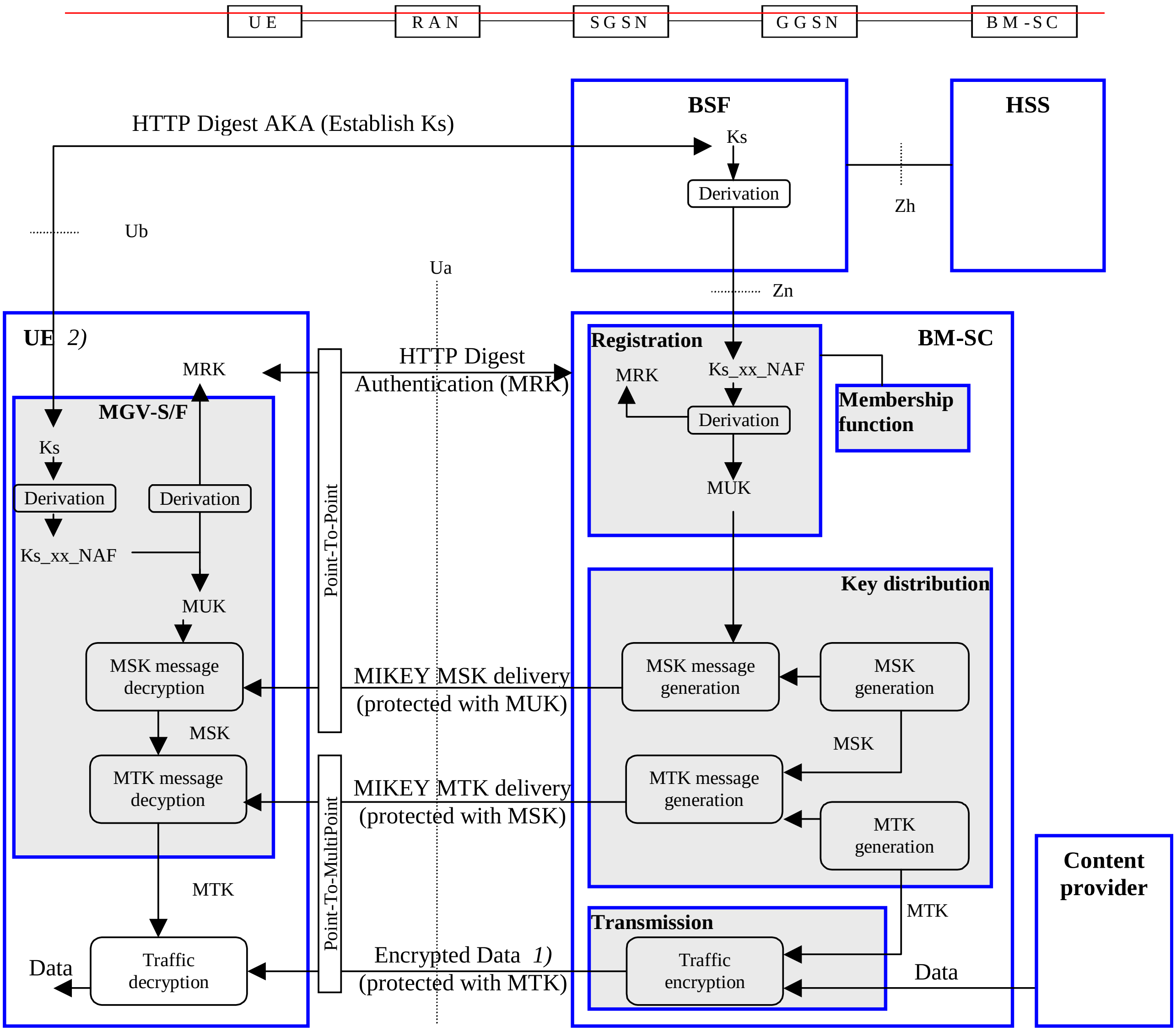
Clauses affected:	⌘	4.1.1 (New), 4.1.2 (New), 4.1.3 (New), 4.2, 5.1, 5.2, 5.3, 6.3.2.2.1, 6.3.2.2.4, 6.3.2.3.1, 6.5.1, 6.6.1, 6.6.2.2,					
		Y	**N**				
Other specs Affected:	⌘	**Y**		Other core specifications	⌘	TS 26.346	
			N	Test specifications			
			N	O&M Specifications			
Other comments:	⌘						

4 MBMS security overview

4.1 MBMS security architecture

4.1.1 General

MBMS introduces the concept of a point-to-multipoint service into a 3GPP system. A requirement of a multicast service is to be able to securely transmit data to a given set of users. In order to achieve this, there needs to be a method of authentication, key distribution and data protection for a multicast service.



Note 1) SRTP is used for streaming and modified DCF format for download

Note 2) Ks_xx_NAF means GBA-ME or GBA_U based NAF keys.

Figure 4.1: MBMS security architecture

Figure 4.1 gives an overview of the network elements involved in MBMS from a security perspective. Nearly all the security functionality for MBMS , ~~(beyond~~except for the normal network bearer security~~)~~ resides in either the BM-SC (Broadcast Multicast – Service Centre) or the UE. The BSF (Bootstrapping Server Function) is a part of GBA (Generic

Bootstrapping Architecture) [6]. The UE and the BM-SC use GBA to establish shared keys that are used to protect the point-to-point communication between the UE and the BM-SC.

The ~~Broadcast Multicast – Service Centre (~~BM-SC~~)~~ is a source for MBMS data. It could also be responsible for scheduling data and receiving data from third parties (this is beyond the scope of the standardisation work) for transmission. ~~It~~ BM-SC is responsible for establishing a shared secret with the UE using GBA, authenticating the UE with HTTP digest authentication mechanism, generating and distributing the keys necessary for ~~multicast~~ MBMS security to the UEs with MIKEY protocol and for applying the appropriate protection to data that is transmitted as part of a MBMS user ~~multicast~~ service. The BM-SC also provides the MBMS bearer authorisation for UEs attempting to establish ~~multicast~~ MBMS bearer..

The UE is responsible for establishing a shared secret with the BM-SC using GBA, requesting and receiving ~~or fetching~~ keys for the ~~multicast~~ MBMS user service from the BM-SC and also using those keys to decrypt the MBMS data that is received.

MBMS imposes the following requirements on the MBMS capable elements:

- 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 as well as providing key management functions itself;
- a BM-SC shall support using GBA_U keys to enable UICC key management.

4.1.2 BM-SC sub-functions

The BM-SC has the following sub-functions related to MBMS security, cf. Figure 4.1.

- **Registration function**: The sub-function is responsible for retrieving GBA keys from the BSF, deriving MUK and MRK from GBA keys, performing initiation of key management and key request procedures and related user authentication using MRK, providing MUK to Key distribution function, performing subscription check from Membership function. The sub-function implements the following security procedures:
    - Bootstrapping initiation
    - Bootstrapping re-negotiation
    - HTTP digest authentication
    - MUK derivation
    - MSK request procedure
- **Key distribution function**: The sub-function is responsible for retrieving MUK from Registration function, generating and distributing MSKs and MTKs to the UE, providing MTK to Session and Transmission function. The sub-function implements the following security procedures:
    - MSK delivery procedure
    - MTK delivery procedure
    - BM-SC solicited pull procedure
- **Session and Transmission function**: As part of other transmission functionality, this function performs protection of data with MTK (encryption and/or integrity protection). The sub-function implements the following security procedures:
    - Protection of streaming data
    - Protection of download content
- **Membership function**: The Membership function is used to verify if a user is authorized to receive keys or to establish a MBMS bearer. The Membership function is defined in [3].

4.1.3 UE security architecture

It is assumed that the UE includes a secure storage (MGV-S). This MGV-S may be realized on the ME or on the UICC but for certain type of MBMS services the UICC shall be used as determined by the service provider. The MGV-F is implemented in a protected execution environment to prevent leakage of security sensitive information such as MBMS keys~~inside MGV-S~~. MGV-S stores the keys and MGV-F performs the functions that should not be exposed to unprotected parts of the ME. An overview of ME based key management and UICC based key management in UE is described in Figure 4.y.

In particular in ME based key management it shall be ensured that the keys are not exposed to unprotected parts of the ME when they are transmitted from the UICC to the MGV-S or during the key derivations.

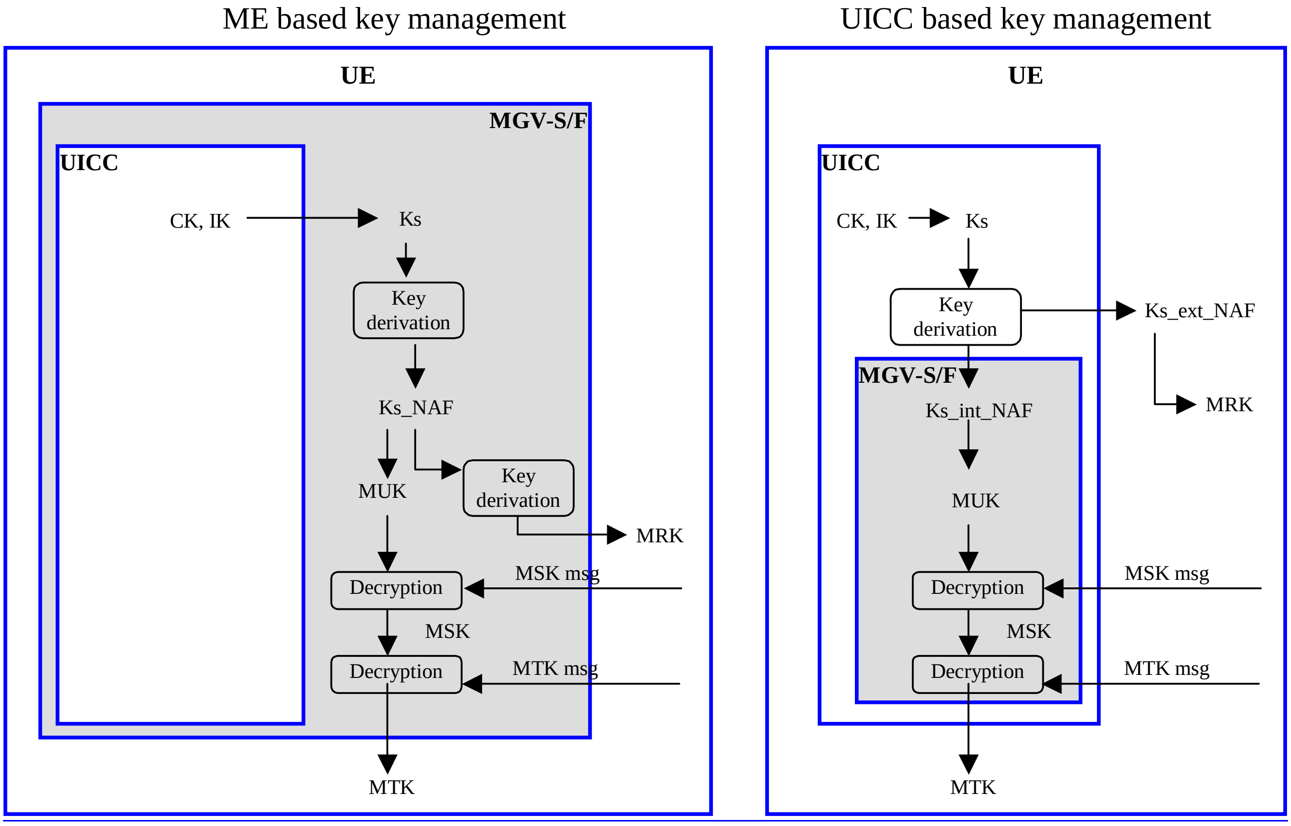


Figure 4.y: ME and UICC based key management in UE

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

4.2 Key management overview

The BM-SC controls the use of the MBMS Service Keys (MSKs) to secure the different MBMS Streaming/Download Sessions that make up the MBMS User Service. The MSKs are not directly used to secure the MBMS Streaming/Download Sessions, but they are used to protect the delivery of MBMS Transport Keys (MTKs), which are used to secure the MBMS Streaming/Download Sessions. as specified within clauses 6.5 and 6.6. MSKs and MTKs are managed at the MBMS User Service Level.

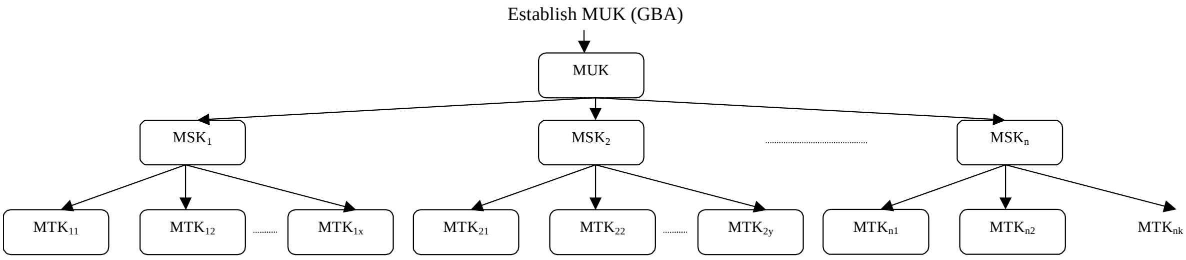


Figure 4.x: MBMS key hierarchy

There shall be only one MSK and MTK in use within one Key Group ID. I.e. parallel use of two or more MSKs (with different MSK IDs) or MTKs (with different MTK IDs) within a Key Group ID shall not be allowed.

The use of the same MTK (this implies also the same MSK) with two different transport services (or user services) should be avoided.

NOTE 1: This is to avoid synchronization problems in the UE when a new MTK is taken into use in the traffic, i.e. if the MTK is not changed synchronously in the traffic flows the UE would discard the traffic with smaller MTK ID.

According to TS 22.246 [5] there exist MBMS User Services with shared and non-shared Transport Services. It shall be possible for MBMS User Services to share one or more MSKs for the shared Transport Services with other MBMS User Services.

NOTE 2: While sharing MSKs among different MBMS User Services, care shall be taken that the Users are not given access to data that they are not entitled to.

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

5 MBMS security functions

5.1 Authenticating and authorizing the user

AUE is authenticated and authorised ~~in the following situations~~ such that only legitimate users ~~when~~ are able to participate~~ing~~ in an MBMS User Service. ~~That is:~~

~~- when the UE performs User Service joining (or leaving) on the application level;~~

~~Editor's Note: The final decision on application level join procedures relies of work in SA4.~~

~~- when the UE establishes (or releases) the MBMS bearer(s) to receive an MBMS User Service;~~

~~- w~~When the UE ~~requests and receives MSKs for the MBMS User Service~~uses HTTP protocol towards the BM-SC, the UE is authenticated with HTTP digest as described in clause 6.2.1. The Membership function within BM-SC is used to verify the subscription information~~;~~

The following procedures use HTTP digest authentication:

- MSK request procedure. This can have many triggers (cf. clause 6.3.2.2).

- Associated delivery procedures (specified in TS 26.346 [13])

When the UE establishes (or releases) the MBMS bearer(s) to receive an MBMS User Service, (cf. clause 6.2.2);

~~- when the UE performs post delivery procedures (e.g. point to point repair service).~~

~~Editor's Note: The final decision on post delivery procedures relies of work in SA4.~~

~~NOTE: The list above does not reflect the order of authentications.~~

5.2 Key derivation, management and distribution

Like any service, the keys that are used to protect the transmitted data in a Multicast service should be regularly changed to ensure that they are fresh. This ensures that only legitimate users can get access to the data in the MBMS service. In particular frequent re-keying acts as a deterrent for an attacker to pass the MBMS keys to others users to allow those other users to access the data in an MBMS service.

The BM-SC is responsible for the generation and distribution of the MBMS keys to the UE. A UE has the ability to request a key when it does not have the relevant key to decrypt the data. This request may also be initiated by a message from the BM-SC to indicate that a new key is available.

The following procedures are involved in Key management and distribution:

- MUK key derivation (clause 6.1)
- MSK request procedure (clause 6.3.2.2)
- MSK delivery procedure (clause 6.3.2.3)
- MTK delivery procedure (clause 6.3.3)
- BM-SC solicited pull (clause 6.3.2.2.4)

5.3 Protection of the transmitted traffic

The traffic for a particular MBMS service may require some protection depending on the sensitivity of the data being transmitted (e.g. it is possible that the data being transmitted by the MBMS service is actually protected by the DRM security method and hence might not require additional protection. However, MBMS protection is independent of DRM protection). If this protection is required, it will be either confidentiality and integrity or confidentiality only, or integrity only. The protection is applied end-to-end between the BM-SC and the UEs and will be based on a symmetric key shared between the BM-SC and the UEs that are currently accessing the service. The actual method of protection specified may vary depending on the type of data being transmitted, e.g. media streaming application or file download.

NOTE: When MBMS data is received over a point-to-point MBMS radio bearer, it would be ciphered between the BM-SC and UE and may also ciphered over the radio interface. This "double ciphering" is unnecessary from a security point of view and hence the decision of whether or not to apply radio interface ciphering to a point-to-point MBMS radio bearer is outside the scope of this specification.

The following procedures are involved in Key management and distribution:

- Protection of streaming data (clause 6.6.2)
- Protection of download content (clause 6.6.3)

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

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 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 procedure is a part of different other procedures, e.g.:

- initiation of key management when the UE has joined the MBMS user service;
- 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.

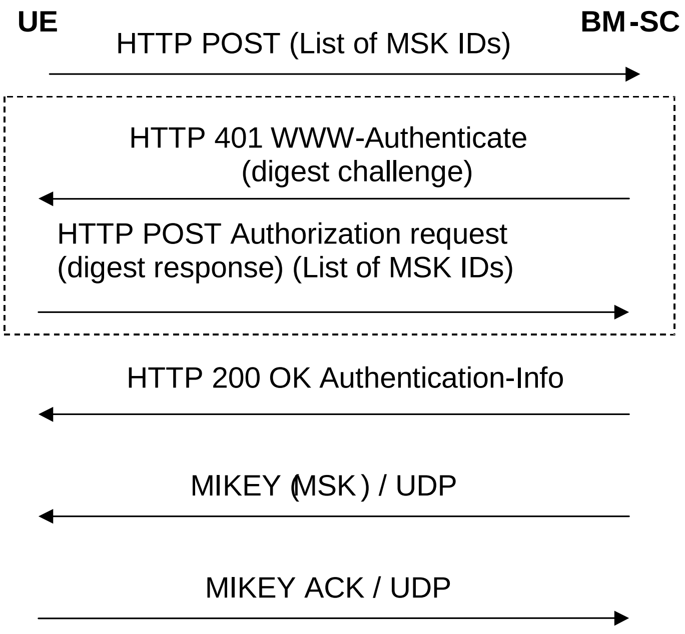

UE
BM-SC
HTTP POST (List of MSK IDs)
HTTP 401 WWW-Authenticate (digest challenge)
HTTP POST Authorization request (digest response) (List of MSK IDs)
HTTP 200 OK Authentication-Info
MIKEY (MSK) / UDP
MIKEY ACK / UDP

Figure 6.1: Basic MSK retrieval procedure

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 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 Registration function authenticates the UE with HTTP Digest using the keys received from GBA as described in clause 6.2.1 and the BM-SC Registration function verifies from the BM-SC Membership function that the subscriber is authorized to receive the MSKs for this service.

If the authentication is successful then the BM-SC Registration function sends a HTTP 200 OK message with Authentication-Info header. If the authentication fails then the BM-SC Registration function 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 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 ****** NEXT CHANGE *******

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 Key Distribution function solicits the UE to contact the BM-SC and request for new MSK. An example of such a situation is when the BM-SC Key Distribution function wants the UE to trigger a UE that it needs to update the MSK.

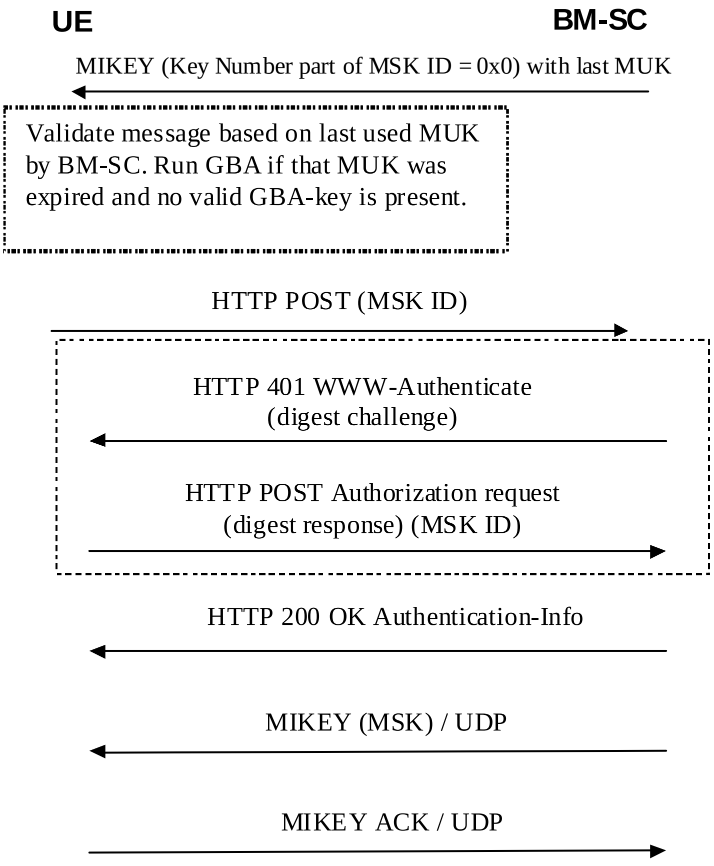

UE
BM-SC
MIKEY (Key Number part of MSK ID = 0x0) with last MUK
Validate message based on last used MUK by BM-SC. Run GBA if that MUK was expired and no valid GBA-key is present.
HTTP POST (MSK ID)
HTTP 401 WWW-Authenticate (digest challenge)
HTTP POST Authorization request (digest response) (MSK ID)
HTTP 200 OK Authentication-Info
MIKEY (MSK) / UDP
MIKEY ACK / UDP

Figure 6.2b: BM-SC solicited pull

The BM-SC Key Distribution function 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 Key Distribution function. 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 Key Distribution function 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 Key Distribution function. 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 Registration function 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 procedures

6.3.2.3.1 Pushing the MSKs to the UE

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

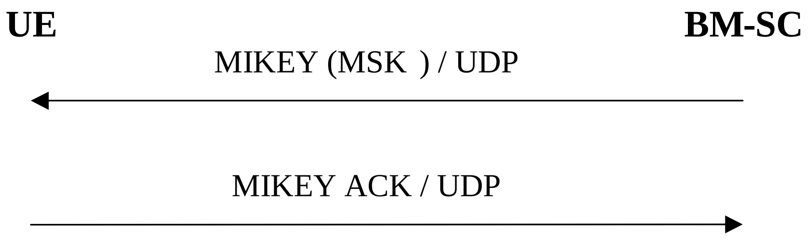


Figure 6.3: Pushing the MSKs to the UE

When the BM-SC Key Distribution function 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 Key Distribution function, the UE sends a MIKEY acknowledgement message to the BM-SC.

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

6.5.1 General

~~It is assumed that the UE includes a secure storage (MGV-S). This MGV-S may be realized on the ME or on the UICC but for certain type of MBMS services the UICC shall be used as determined by the service provider. The MGV-F is implemented inside MGV-S.~~

Editor's Note: The choice between MIKEY key derivation algorithms and other suitable key derivations has not been made as there could be algorithms already in the UE.

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

6.6.1 General

The data transmitted to the UEs is protected by a symmetric key (an MTK) that is shared by the BM-SC and UEs that are accessing the MBMS service. The protection of the data is applied by the BM-SC Session and Transmission Function. In order to determine which key was used to protect the data key identification information is included with the protected data. The key identification information will uniquely identify the MSK and MTK. The MTK is processed according to the methods described in clauses 6.4 and 6.5. Whenever data from an MBMS User Service has been decrypted, if it is to be stored on the UE it will be stored decrypted.

NOTE: Including the key identification information with the protected data stops the UE trying to decrypt and render content for which it does not have the MSK.

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

6.6.2.2 Packet processing in the UE

When the SRTP module in BM-SC Session and Transmission Function receives a packet, it will retrieve the correct cryptographic context identified by destination transport address, destination port and SSRC (according to RFC 3711 [11]), check if it has the MTK corresponding to the value in the MKI field in the SRTP cryptographic context.

NOTE 1: The cryptographic context needs to be unique for each SRTP stream.

NOTE 2: The SRTP module does not need to interpret the MKI field semantics. It only checks whether it has the MTK corresponding to the MKI value.

If the check is successful, the SRTP module processes the packet according to the security policy.

If the SRTP module does not have the MTK, it will request the MTK corresponding to the MKI from the key management module. When the key management module returns a new MTK, the SRTP module will derive new session keys from the MTK and process the packet. However, if the key management module does not have the MSK indicated by MKI, then it should fetch the MSK using the methods discussed in the clause 6.3.

If the correct MTK is not present in the UE when RTP traffic arrives, the UE shall wait for the next MTK update procedure from the BM-SC as described in clause 6.3.3.2.

NOTE 3: It is implementation specific issue whether the UE spools encrypted packets or discards all packets before the UE has received the correct MTK.

If the SRTP module has lost synchronisation on the ROC (Roll-over counter) of the SRTP stream, it shall wait for the next MTK update message received within the ptm stream. The BM-SC shall deliver the current ROC-value within the CS ID map info payload of the MIKEY common header payload.

The below flow shows how the protected content is delivered to the UE.

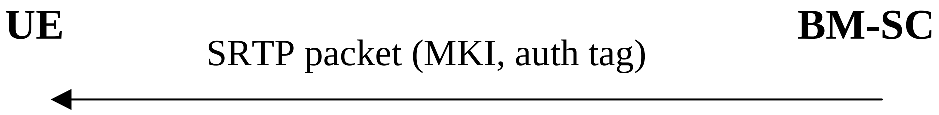


Figure 6.8: Delivery of protected streaming content to the UE