3GPP TSG SA WG3 Security — S3#37 **S3-050131**
21 - 25 February 2005
Sophia Antipolis, France

Title: LS on 'MBMS security functions, procedures and Architecture'
Response to: LS S3-050008 (S4-040760): Reply on "LS on MBMS Security finalisation"
Release: Rel-6
Work Item: MBMS

Source: SA3
To: SA4
Cc: ----

Contact Person:
Name: Blommaert Marc
Tel. Number: +32 14 25 34 11
E-mail Address: Marc.Blommaert@siemens.com

Attachments: S3-050124, S3-040130, S3-040134

1. Overall Description

SA3 thanks SA4 for their Reply LS on "MBMS Security finalisation" (S4-040760).

SA3 have discussed S4-040859 (TS 26.346 V150) Section 4.4 on 'Functional Entities to support MBMS User Services'. With regard to the naming of security functions within Figure 4 (BM-SC sub-functional structure), SA3 have following proposals for renaming:

1) rename 'Security Function' to 'Key Management Function'.
2) rename 'Registration Function' to 'Key Request Function'.

It was noted during SA3-plenary discussion that the description of the current security function in section 4.4.2 includes a sentence on confidentiality and integrity protection. This functionality does better belong to section on 4.4.3 on 'MBMS Session and Transmission Function' , but does not need a separate functional box in figure 4. Hence SA3 have following concrete proposals (See change bars) to clarify section 4.4.2 and 4.4.3 related security text:

4.4.2 MBMS Key Management ~~Security~~ Function

~~MBMS user services may use security functions for integrity and/or confidentiality protection of MBMS data.~~ The MBMS Key Management ~~security~~ function is used for distributing MBMS keys (Key Distribution subf~~F~~unction) to authorized UEs. Before the UE can receive MBMS keys, the UE needs to register to the Key Request subfunction of the Key Management function by indicating the MBMS User Service Id. Once registered, the UE can request missing MBMS keys to the BM-SC by indicating the specific MBMS key id. In order for the UE to stop the BM-SC to send MBMS key updates a deregistration with the MBMS User Service Id is needed.

If the MBMS User Service does not require any MBMS data protection, then the UE shall not register for key management purposes.

~~UEs request the initial keys from the BM-SC and register (using the Registration Function) to receive key updates by key management procedures.~~ A Detailed description of all key management procedures ~~the security functions~~ is provided in TS 33.246 [20] ~~(TS 33.246)~~.

~~[Editor's Note: The MBMS Security function is to be confirmed by SA3]~~

4.4.3 MBMS Session and Transmission Function

The MBMS Session and Transmission function transfers the actual MBMS session data to the group of MBMS UEs. The MBMS Session and Transmission function interacts with the GGSN through the Gmb Proxy function to activate and release the MBMS transmission resources.

The function contains the MBMS delivery methods, which use the MBMS bearer service for distribution of content. Further this function contains a set of Associated-Delivery Functions, which may be invoked by the UE in relation to the MBMS data transmission (e.g. after the MBMS data transmission).
The BM-SC Session and Transmission function is further described in later clauses of this specification as well as in TS 23.246 [4] ~~(TS 23.246)~~.
MBMS user services data may be integrity and/or confidentiality protected as specified within TS 33.246 [20], and protection is applied between the BM-SC and the UE.
~~If security functions are activated for the MBMS User Service, the confidentiality and/or integrity protection is applied by the BM-SC to outgoing MBMS data transmissions. The traffic protection is applied between the BM-SC and the UEs.~~ This data protection~~e~~ ~~security~~ is based on symmetric keys, which are shared between the BM-SC and the UEs accessing the service. ~~For further details on traffic protection see [20] (TS 33.246)~~.

~~[Editor's Note: The MBMS Security function is to be confirmed by SA3].~~

Attached there are two agreed SA3#37 change requests: S3-050130 (Clarification of HTTP procedures) and S3-050134 (Introduction of BM-SC subfunctions) which implement the above proposed 'security functions' names and the required key management procedures within the TS 33.246.

Additionally, SA3#37 agreed on a CR (S3-05124) about protection of Service Announcements sent over MBMS Bearer.

2. Actions

ACTION: SA3 kindly asks SA4

1. to align TS 26.346 with the attached CR's and the proposal above for Section 4.4.2 and 4.4.3 of TS 26.346
2. to provide comments if there would be problems with the implementation of these within TS 26.346.
3. to specify the MIME types which are needed for MSK request and MBMS User Service Registration/Deregistration, as described in Annex F of S3-050130.

3. Date of Next TSG-SA3 Meetings

SA3#38	26 – 29 April 2005 Geneva, Switzerland
SA3#39	28 June- 1 July Toronto, Canada

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

Tdoc ⌘S3-050124

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**056**	⌘**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:	⌘	Protection of MBMS Service Announcement sent over MBMS bearer		
Source:	⌘	MBMS drafting group		
Work item code:	⌘	MBMS	***Date:*** ⌘	22/02/2005
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 considered not practical to protect service announcements in case they are sent over MBMS Bearer.
Summary of change:	⌘	The service announcements are not protected.
Consequences if not approved:	⌘	It is not specified whether MBMS service announcements are protected.

Clauses affected:	⌘	6.3.2.2.2, B.1				
		Y	N			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

===== BEGIN CHANGE =====

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.

NOTE1: 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.

NOTE2: The user service announcements are not protected when sent over MBMS bearer.

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.

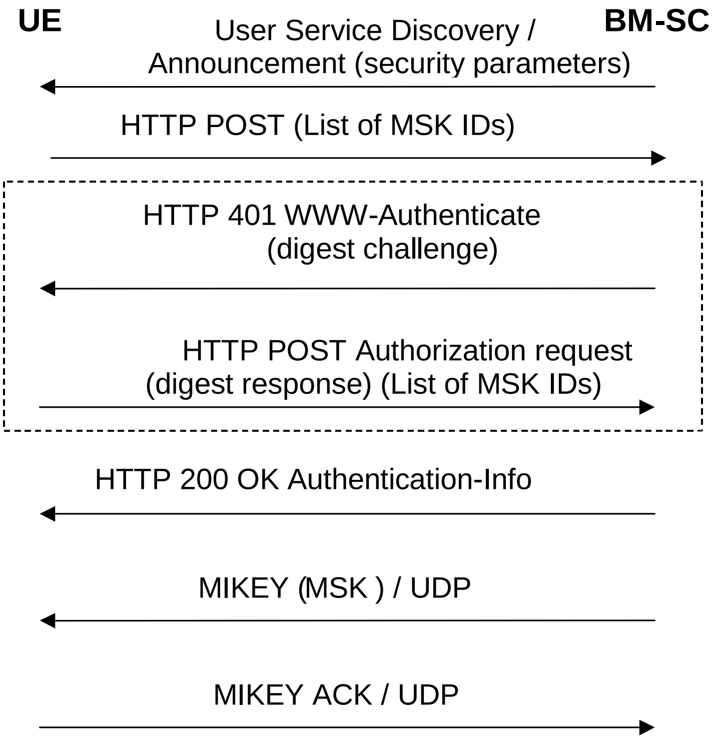

UE
BM-SC
User Service Discovery / Announcement (security parameters)
HTTP POST (List of MSK IDs)
HTTP 401 WWW-Authenticate (digest challenge)
HTTP POST Authorization request (digest response) (List of MSK IDs)
HTTP 200 OK Authentication-Info
MIKEY (MSK) / UDP
MIKEY ACK / UDP

Figure 6.2a: 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 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.

===== NEXT CHANGE =====

Annex B (informative): Security threats

B.1 Threats associated with attacks on the radio interface

The threats associated with attacks on the radio interface are split into the following categories, which are described in the following clauses:

- unauthorized access to multicast data;
- threats to integrity;
- denial of service;
- unauthorized access to MBMS services;
- privacy violation.

The attacks on the MBMS service announcements to the users on the radio interface are not discussed here~~,~~ because in case~~as~~ these are~~will most likely be~~ transferred on a point-to-point connection (e.g. PS signaling connection) they are~~, which is~~ already secured~~ today~~. In case the service announcement is transferred over HTTP, it is protected by HTTP Digest as defined in the current specification and/or it may be ~~(~~integrity protected and optionally encrypted at the RAN level~~)~~. In case the service announcements are sent over MBMS bearer, it is impractical to protect them.

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

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

Tdoc ⌘S3-050130

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**044**	⌘**rev**	**1**	⌘	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:	⌘	Clarification of HTTP procedures		
Source:	⌘	SA WG3		
Work item code:	⌘	MBMS	***Date:*** ⌘	23/2/2005
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:	⌘	The details of HTTP procedures for MSK request have not been specified for MBMS security. In addition HTTP digest authentication has been underspecified.
Summary of change:	⌘	The details of HTTP procedures are added as annexes to 33.246. This includes details for MBMS User Service Registration, MBMS User Service Deregistration and MSK request procedures. It is proposed that the definition of HTTP payload in XML is specified in SA4 TS 26.346. HTTP digest authentication is clarified and necessary references are added to TS 24.109 for applicable parts that describe the details of HTTP digest authentication. In addition, all text regarding application level joining is removed since SA4 TS does not have such procedure.
Consequences if not approved:	⌘	HTTP procedures will remain underspecified and unclear.

Clauses affected:	⌘	2, 6.2, 6.2.1, 6.2.1.1-6.2.1.3 (new), 6.2.3, 6.2.4, 6.3, 6.3.1, 6.3.2.2.1, Annex F (new), Annex G (new)					
		Y	**N**				
Other specs Affected:	⌘	**Y**		Other core specifications	⌘	TS 26.346	
			N	Test specifications			
			N	O&M Specifications			

Other comments:	⌘

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

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: "Multimedia Broadcast/Multicast Service; Protocols and Codecs".

[14] 3GPP TS 33.210: "Network domain security; IP network layer security".

[15] OMA-DRM-DCF-v2_0: "OMA DRM Content Format", www.openmobilealliance.org

[16] IETF internet draft: "The Key ID Information Type for the General Extension Payload in MIKEY" <draft-carrara-newtype-keyid-00.txt>.

[xx] 3GPP TS 24.109: "Bootstrapping interface Ub and network application function interface Ua".

[yy] IETF RFC 2616 " Hypertext Transfer Protocol -- HTTP/1.1".

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

6.2 Authentication and authorisation of a user

Editor's Note: The exact details on how to derive the keys MRK and MUK from the GBA keys are for ffs.

~~Editor's Note: According to S3-040212, SA4 has a working assumption to use HTTP as the transport protocol but this is only agreed for the download repair service.~~

6.2.1 Authentication and authorisation in ~~application level joining~~HTTP procedures

6.2.1.1 General

This chapter describes authentication when using HTTP digest with bootstrapped security associations.

6.2.1.2 Bootstrapping

The BM-SC shall implement Bootstrapping procedure over Ub, Initiation of bootstrapping and Bootstrapping renegotiation procedures over Ua as specified in TS 33.220 [6] and in clause 4 and clause 5.2 of TS 24.109 [xx]. The Ua interface procedures shall use MRK.

6.2.1.3 HTTP digest authentication

When the ~~user wants to join (or leave) an MBMS user service~~UE initiates an HTTP procedure towards the BM-SC, ~~it shall use~~ HTTP digest authentication as defined in RFC 2617 [8] shall be used for mutual authentication. HTTP digest is run between BM-SC and ME. The MBMS authentication procedure is based on the general user authentication procedure over Ua interface that is specified in clause "Procedures using the bootstrapped Security Association" in TS 33.220 [6]. The BM-SC will act as a NAF according to TS 33.220 [6]. The details of HTTP digest authentication are specified in clause 5.2 of [xx].

The following adaptations apply to HTTP digest:

- the ~~transaction identifier~~B-TID as specified in TS 33.220 [6] is used as username;
- MRK (MBMS Request Key) is used as password;
- ~~the joined MBMS user service is specified in client payload of~~

All HTTP ~~Digest message~~ procedures within this specification including the associated delivery procedures in TS 26.346 [13] shall be integrity protected with HTTP digest as specified in this clause.

~~Editor's Note: The contents of the client payload are FFS and may require input from TSG SA WG4. The final decision on application level join and leave procedures relies of work in SA4.~~

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

6.2.3 Void~~Authentication and authorisation in MSK request~~

~~When the UE requests MSK(s), the UE shall be authenticated with HTTP digest as in clause 6.2.1.~~

6.2.4 Void~~Authentication and authorisation in post delivery procedures~~

~~When the UE requests post delivery procedures, the UE shall be authenticated with HTTP digest as in clause 6.2.1.~~

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

6.3 Key update procedures

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

6.3.1 General

In order to protect an MBMS User service, it is necessary to transfer both MSKs and MTKs from the BM-SC to the UE. Clause 6.3.2 describes the possible procedures for transferring MSKs, while clause 6.3.3 deals with the transfer of MTKs.

The details of the HTTP procedures and HTTP error situations are specified in Annex F. An example of detailed MSK request procedure is described in Annex G. The XML schema of the HTTP payload is specified in [13].

******* 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.

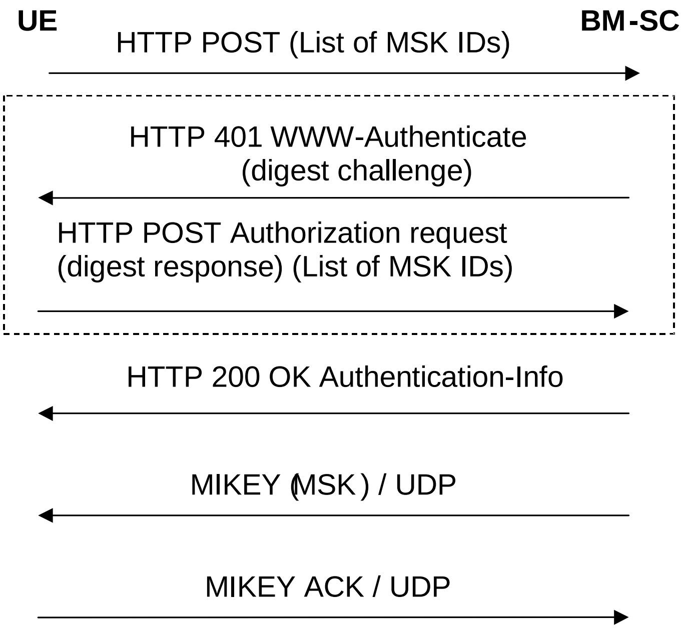

UE
BM-SC
HTTP POST (List of MSK IDs)
HTTP 401 WWW-Authenticate (digest challenge)
HTTP POST Authorization request (digest response) (List of MSK IDs)
HTTP 200 OK Authentication-Info
MIKEY (MSK) / UDP
MIKEY ACK / UDP

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~~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~~ TS 26.346 [13].

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.

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 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.

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

Annex F (Normative):
HTTP based key management messages

F.1 Introduction

Section 6 specifies the HTTP based key management procedures between the BM-SC and the UE. It specifies that the authentication of these procedures is based on GBA and more specifically on the HTTP Digest authentication as described in clause 6.2 of the present document.

F.2 Key management procedures

This clause contains the following HTTP based procedures:

- MBMS User Service Registration;
- MBMS User Service Deregistration;
- MSK request;

F.2.1 MBMS User Service Registration

The UE shall generate a request for MBMS User Service Registration according to clause 6.3.x.x. The UE shall send the Registration request to the BM-SC in the HTTP payload in a HTTP POST request. The Request-URI shall indicate the type of the message, i.e. Registration request. Upon successful request, BM-SC shall return indication of success.

The UE populates the HTTP POST request as follows:

- the HTTP version shall be 1.1 which is specified in RFC 2616 [yy];
- the base of the Request-URI shall contain the full BM-SC key management URI (e.g. http://bmsc.home1.net/keymanagement)
- the Request-URI shall contain an URI parameter "requesttype" that shall be set to "register", i.e. Request-URI takes the form of " /bmsc.home1.net/keymanagement?requesttype= register”
- the UE may add additional URI parameters to the Request-URI;
- the HTTP header Content-Type shall be the MIME type of the payload, e.g. "application/vnd.3gpp.mbms-register+xml ". The XML schema of payload is specified in TS 26.346 [13];
- the HTTP header Content-Length shall be the length of the Base64 encoded Register request in octets; and
- the HTTP payload shall contain the Base64 encoded Register request including the userServiceId of MBMS User Service to which the UE wants to register;
- the UE may add additional HTTP headers to the HTTP POST request.

The UE sends the HTTP POST to the BM-SC. The BM-SC checks that the HTTP POST is valid, and extracts the Base64 encoded Register request for further processing. The BM-SC Key Management function shall verify from BM-SC Membership function that the subscriber is authorized to register to the particular MBMS User Service.

Upon successful authorization verification, the BM-SC shall return the HTTP 200 OK to the UE.

The BM-SC shall populate HTTP response as follows:

- the HTTP status code shall be 200

The BM-SC shall send the HTTP response to the UE. The UE shall check that the HTTP response is valid.

F.2.2 MBMS User Service Deregistration

The UE shall generate a request for MBMS User Service Deregistration according to clause 6.3.x.x. The UE shall send the Deregistration request to the BM-SC in the HTTP payload in a HTTP POST request. The Request-URI shall indicate the type of the message, i.e. Deregistration request. Upon successful request, BM-SC shall return indication of success.

The UE populates the HTTP POST request as follows:

- the HTTP version shall be 1.1 which is specified in RFC 2616 [yy];
- the base of the Request-URI shall contain the full BM-SC key management URI (e.g. http://bmsc.home1.net/keymanagement)
- the Request-URI shall contain an URI parameter "requesttype" that shall be set to "deregister", i.e. Request-URI takes the form of " /bmsc.home1.net/keymanagement?requesttype= deregister”
- the UE may add additional URI parameters to the Request-URI;
- the HTTP header Content-Type shall be the MIME type of the payload, e.g. "application/vnd.3gpp.mbms-deregister+xml ". The XML schema of payload is specified in TS 26.346 [13];
- the HTTP header Content-Length shall be the length of the Base64 encoded Deregister request in octets; and
- the HTTP payload shall contain the Base64 encoded Deregister request including the userServiceId of MBMS User Service from which the UE wants to deregister;

- the UE may add additional HTTP headers to the HTTP POST request.

The UE sends the HTTP POST to the BM-SC. The BM-SC checks that the HTTP POST is valid, and extracts the Base64 encoded Deregister request for further processing.

Upon successful authorization verification, the BM-SC shall return the HTTP 200 OK to the UE.

The BM-SC shall populate HTTP response as follows:

- the HTTP status code shall be 200

The BM-SC shall send the HTTP response to the UE. The UE shall check that the HTTP response is valid.

F.2.3 MSK request

The UE shall generate a MSK request according to clause 6.3.2.2. The UE shall send the MSK request to the BM-SC in the HTTP payload in a HTTP POST request. The Request-URI shall indicate the type of the message, e.g. MSK request. Upon successful request, BM-SC shall return indication of success.

The UE populates the HTTP POST request as follows:

- the HTTP version shall be 1.1 which is specified in RFC 2616 [yy];
- the base of the Request-URI shall contain the full BM-SC key management URI (e.g. http://bmsc.home1.net/keymanagement)
- the Request-URI shall contain an URI parameter "requesttype" that shall be set to "msk-request", i.e. Request-URI takes the form of " /bmsc.home1.net/keymanagement?requesttype= msk-request”
- the UE may add additional URI parameters to the Request-URI;
- the HTTP header Content-Type shall be the MIME type of the payload, e.g. "application/vnd.3gpp.mbms-msk+xml ". The XML schema of payload is specified in TS 26.346 [13];
- the HTTP header Content-Length shall be the length of the Base64 encoded MSK request in octets; and
- the HTTP payload shall contain the Base64 encoded MSK request;
- the UE may add additional HTTP headers to the HTTP POST request.

The UE sends the HTTP POST to the BM-SC. The BM-SC checks that the HTTP POST is valid, and extracts the Base64 encoded MSK request for further processing. The BM-SC Key Management function shall verify from the BM-SC Membership function that the subscriber is authorized to receive the particular MSKs.

Upon successful authorization verification, the BM-SC shall return the HTTP 200 OK to the UE.

The BM-SC shall populate HTTP response as follows:

- the HTTP status code shall be 200

The BM-SC shall send the HTTP response to the UE. The UE shall check that the HTTP response is valid.

An example flow of a successful MSK request procedure can be found in Annex G.

F.2.4 Error situations

The key management procedures may not be successful for multiple reasons. The error cases are indicated by using 4xx and 5xx HTTP Status Codes as defined in RFC 2616 [yy]. The 4xx status code indicates that the UE seems to have erred, and the 5xx status code indicates that the BM-SC is aware that it has erred. Possible error situations during key management and their mappings to HTTP Status Codes are described in table F.2.4-1.

NOTE: In table F.2.4-1, the "Description" column describes the error situation in BM-SC. The "BM-SC error" column describes the typical reason for the error.

Table F.2.4-1: HTTP Status Codes used for key management errors

HTTP Status Code	HTTP Error	UE should repeat the request	Description	BM-SC error
400	Bad Request	No	Request could not be understood	Request was missing, or malformed
401	Unauthorized	Yes	Request requires authentication (cf. clause 6.2)	Authentication pending, (cf. clause 6.2)
402	Payment Required	No	Reserved for future use	-
403	Forbidden	No	BM-SC understood the request, but is refusing to fulfil it	The request was valid, but subscriber is not allowed to register to this particular MBMS User Service or UE requested MSK for a MBMS User Service where it was not registered or request contained unacceptable parameters
404	Not Found	No	BM-SC has not found anything matching the Request-URI	The Request-URI was malformed and BM-SC cannot fulfil the request
405	Method not allowed	No	The method specified in the Request-Line is not allowed for the resource identified by the Request-URI.	
406 to 417	*	No	Not used by BM-SC	-
500	Internal Server Error	No	Not used by BM-SC	-
501	Not Implemented	No	BM-SC does not support the requested functionality	The server does not contain particular BM-SC service requested
502	Bad Gateway	No	Not used by BM-SC	-
503	Service Unavailable	Yes	BM-SC service is currently unavailable	BM-SC is temporarily unavailable, UE may repeat the request after delay indicated by "Retry-After" header
504	Gateway Timeout	No	The server, while acting as a gateway or proxy, did not receive a timely response from the upstream server	The BM-SC did not get response over Zn interface.
505	HTTP Version Not Supported	No	BM-SC does not support the HTTP protocol version that was used in the request line	UE should use HTTP/1.1 version with BM-SC

Annex G (Informative): Signalling flows for MSK procedures

G.1 Scope of signalling flows

This annex gives examples of signalling flows for the key management procedures.

G.2 Signalling flows demonstrating a successful MSK request procedure

G.2.1 Successful MSK request procedure

The signalling flow in figure G.2.1-1 describes the message exchange between UE and BM-SC when UE wants to request MSK.

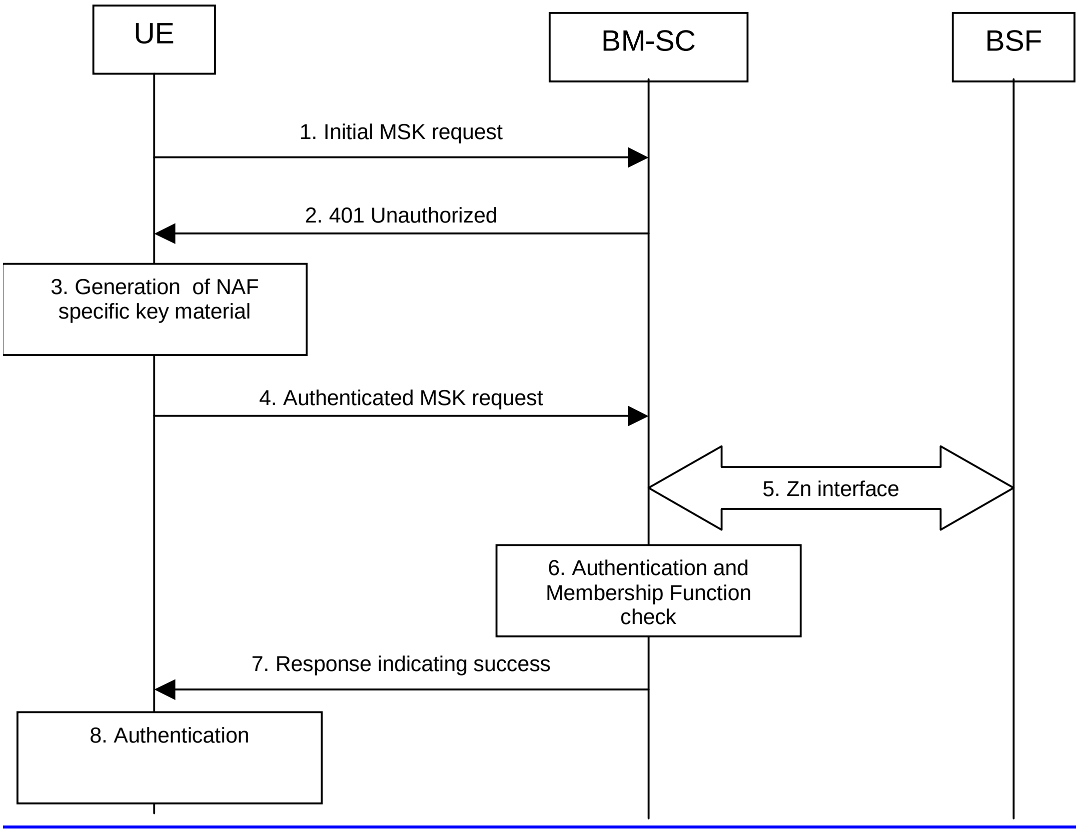

UE
BM-SC
BSF
1. Initial MSK request
2. 401 Unauthorized
3. Generation of NAF specific key material
4. Authenticated MSK request
5. Zn interface
6. Authentication and Membership Function check
7. Response indicating success
8. Authentication

Figure G.2.1-1: Successful MSK request procedure.

1. **Initial MSK request (UE to BM-SC) - see example in table G.2.1-1**

   The UE sends an HTTP request to the BM-SC containing a MSK request.

Table G.2.1-1: MSK request (UE to BM-SC)

```
POST /bmsc.home1.net/keymanagement?requesttype=msk-request HTTP/1.1
Host: bmsc.home1.net:1234
Content-Type: application/vnd.3gpp.mbms-msk+xml
Content-Length: (...)
```

```
User-Agent: MBMSAgent; Release-6 3gpp-gba
Date: Thu, 08 Jan 2004 10:50:35 GMT
Accept: */*
Referrer: http://bmsc.home1.net:1234/service

<MSK request BLOB>
```

Request-URI: The Request-URI (the URI that follows the method name, "POST", in the first line) indicates the resource of this POST request. The Request-URI contains the parameter "requesttype " which is set to "msk-request " to indicate to the BM-SC the desired request type, i.e. UE requests for one or several MSKs.

Host: Specifies the Internet host and port number of the BM-SC, obtained from the original URI given by referring resource.

Content-Type: Contains the media type " application/vnd.3gpp.mbms-msk+xml ", i.e. MSK request.

Content-Length: Indicates the size of the entity-body, in decimal number of OCTETs, sent to the recipient.

User-Agent: Contains information about the user agent originating the request and it shall include the static string "3gpp-gba" to indicate to the application server (i.e., NAF) that the UE supports 3GPP-bootstrapping based authentication.

Date: Represents the date and time at which the message was originated.

Accept: Media types which are acceptable for the response.

Referer: Allows the user agent to specify the address (URI) of the resource from which the URI for the BM-SC was obtained.

NOTE 1: This step is used to trigger the GBA-based authentication between the UE and the BM-SC.

2. **401 Unauthorized response (BM-SC to UE) - see example in table G.2.1-2**

Upon receiving an HTTP request that contains static string "3gpp-gba" in the User-Agent header the BM-SC responds with HTTP response code 401 "Unauthorized" which contains a WWW-Authenticate header. The header instructs the UE to use HTTP Digest Authentication with a bootstrapped security association.

Table G.2.1-2: 401 Unauthorized response (BM-SC to UE)

```
HTTP/1.1 401 Unauthorized
Server: Apache/1.3.22 (Unix) mod_perl/1.27
Date: Thu, 08 Jan 2004 10:50:35 GMT
WWW-Authenticate: Digest realm="3GPP-bootstrapping@bmsc.home1.net",
nonce="6629fae49393a05397450978507c4ef1", algorithm=MD5, qop="auth,auth-int",
opaque="5ccc069c403ebaf9f0171e9517f30e41"
```

Server: Contains information about the software used by the origin server (BM-SC).

Date: Represents the date and time at which the message was originated.

WWW-Authenticate: The BM-SC challenges the user. The header instructs the UE to use HTTP Digest Authentication with a bootstrapped security association.

The options for the quality of protection (qop) attribute is by default "auth-int" meaning that the payload of the following HTTP requests and responses should be integrity protected.

The realm attribute contains two parts delimited by "@" sign. The first part is a constant string "3GPP-bootstrapping" instructing the UE to use a bootstrapped security association. The second part is the hostname of the server (i.e. FQDN of the BM-SC).

3. **Generation of NAF specific keys at UE**

The UE verifies that the second part of the realm attribute does correspond to the server it is talking to.

UE derives the NAF specific key material as specified in 3GPP TS 33.220 [6]. UE further derives MBMS specific key material MRK and MUK as specified in clause 6.1.

NOTE 2: If UE does not have a bootstrapped security association available, it will obtain one by running bootstrapping procedure over Ub interface.

4. Authenticated MSK request (UE to BM-SC) - see example in table G.2.1-3

UE generates the HTTP request by calculating the Authorization header values using the bootstrapping transaction identifier B-TID it received from the BSF as the username and the MRK (base64 encoded) as the password, and sends the request to BM-SC.

Table G.2.1-3: Authenticated enrolment request (UE to BM-SC)

```
POST /bmsc.home1.net/keymanagement?requesttype=msk-request HTTP/1.1
Host: bm.sc.home1.net:1234
Content-Type: application/vnd.3gpp.mbms-msk+xml
Content-Length: (...)
User-Agent: MBMSAgent; Release-6 3gpp-gba
Date: Thu, 08 Jan 2004 10:50:35 GMT
Accept: */*
Referer: http://bmsc.home1.net:1234/service
Authorization: Digest username="(B-TID)", realm="3GPP-bootstrapping@bmsc.home1.net",
nonce="a6332ffd2d234==", uri="/bmsc.home1.net/keymanagement?requesttype=msk-request”, qop=auth-int,
nc=00000001, cnonce="6629fae49393a05397450978507c4ef1", response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f30e41", algorithm=MD5

<MSK request BLOB>
```

Authorization: This carries the response to the authentication challenge received in step 2 along with the username, the realm, the nonce, the URI, the qop, the NC, the cnonce, the response, the opaque, and the algorithm.

The qop attribute is set to "auth-int" by default.

NOTE 3: If step 1 was a POST request then this request would also be a POST request and contain the same client payload in the HTTP request as was carried in step 1.

5. Zn: NAF specific key procedure

BM-SC retrieves the NAF specific key material. BM-SC further derives MBMS specific key material MRK and MUK as specified in clause 6.1.

For detailed signalling flows see 3GPP TS 29.109 [xx].

Table G.2.1-4: Bootstrapping authentication information procedure (BM-SC to BSF)

Message source and destination	Zn Information element name	Information Source in GET	Description
NAF to BSF	B-TID	Authorization	The bootstrapping transaction identifier is encoded in the username field according to the Authorization protocol.

6. Authentication and certificate generation at BM-SC

BM-SC verifies the Authorization header by using the bootstrapping transaction identifier B-TID and the key MRK. BM-SC calculates the corresponding digest values using MRK, and compares the calculated values with the received values in the Authorization header.

The BM-SC also verifies that the hostname (i.e. its FQDN) in the realm attribute matches its own.

If the verification succeeds, the incoming client-payload request is taken in for further processing. The BM-SC continues processing of the MSK request according to its internal policies. The BM-SC verifies that the subscriber is allowed to receive the particular MSK(s) indicated in the MSK request by checking the BM-SC Membership function.

7. **Response indicating success (BM-SC to UE) - see example in table G.2.1-5**

The BM-SC sends 200 OK response to the UE to indicate the success of the authentication and the MSK request. The BM-SC generates a HTTP response. The BM-SC can use key MRK derived from NAF key material to integrity protect and authenticate the response.

NOTE 5: The requested MSK keys are not delivered within the MSK request procedure. They are delivered with a separate MIKEY procedure, see clause 6.3.2.3.

Table G.2.1-5: Successful HTTP response (BM-SC to UE)

```
HTTP/1.1 200 OK
Server: Apache/1.3.22 (Unix) mod_perl/1.27
Authentication-Info: qop=auth-int, rspauth="6629fae49394a05397450978507c4ef1",
cnonce="6629fae49393a05397450978507c4ef1", nc=00000001
Date: Thu, 08 Jan 2004 10:50:35 GMT
Expires: Fri, 09 Jan 2004 10:50:36 GMT
```

Authentication-Info: This carries the protection

Expires: Gives the date/time after which the response is considered stale.

8. **Authentication at UE**

The UE receives the response and verifies the Authentication-Info header. If the verification succeeds, the UE can regard the MSK request procedure as successful.

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

Tdoc ⌘S3-050134

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**052**	⌘**rev**	**1**	⌘	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:	⌘	SA WG3		
Work item code:	⌘	MBMS	***Date:*** ⌘	23/2/2005
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:	⌘	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 is added to describe the MBMS security sub-functions. The Security architecture is clarified.
Consequences if not approved:	⌘	The specification will not be aligned with SA4 TS 26.346.

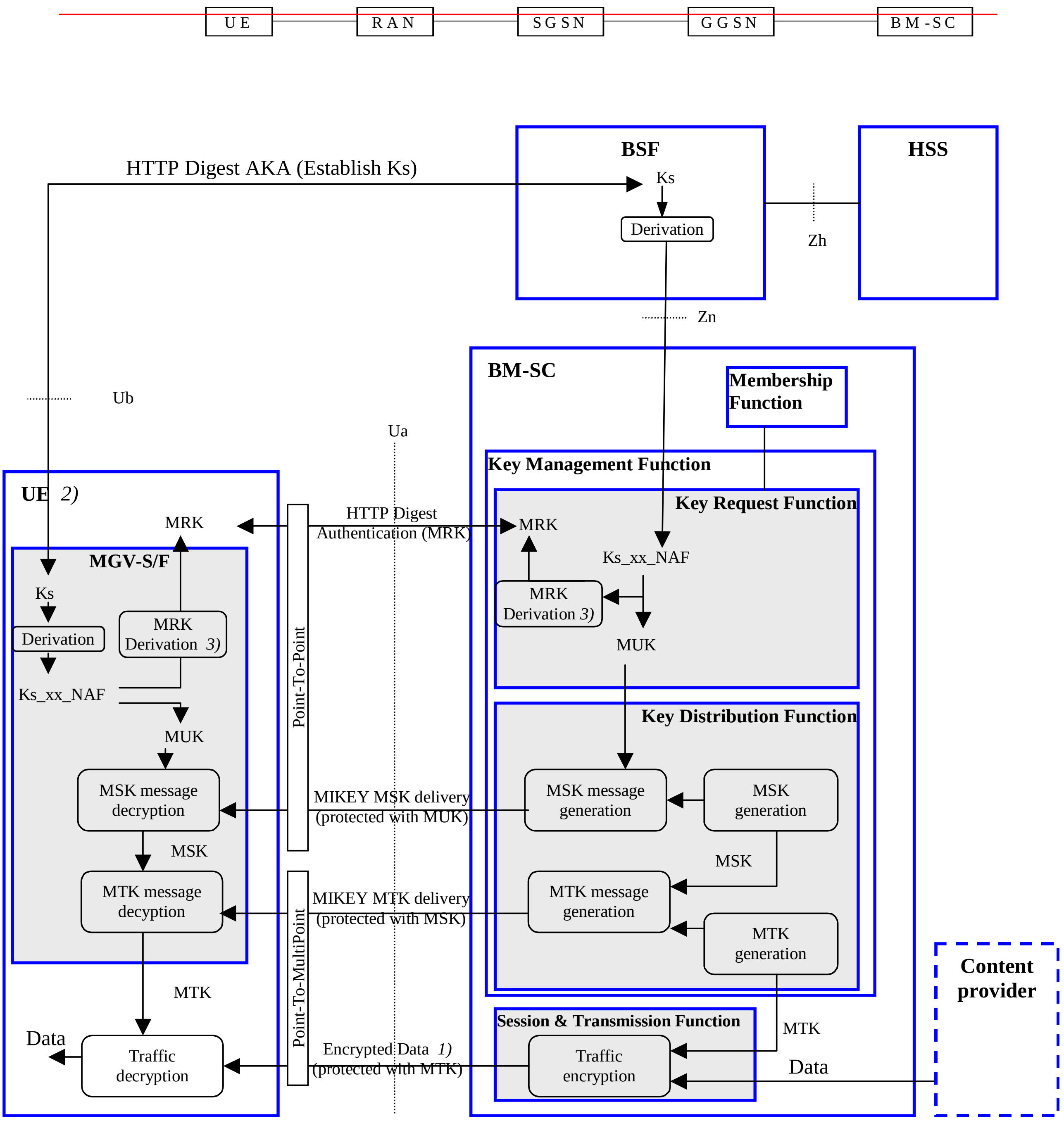
Clauses affected:	⌘	4.1.1 (New), 4.1.2 (New), 4.1.3 (New), 4.2, 5.1, 5.2, 5.3				
		Y	**N**			
Other specs Affected:	⌘	**Y**		Other core specifications	⌘	TS 26.346
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

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 stands for GBA_ME or GBA_U based NAF keys

Note 3) Not applicable for GBA_U, since MRK=Ks_ext_NAF

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 or the UE. The BSF is a part of GBA [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 shared secrets with the UE using GBA, authenticating the UE with HTTP digest authentication mechanism, registering and de-registering UEs for MBMS User Services, 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 shared secrets with the BM-SC using GBA, registering to, and de-registering from, MBMS User Services, 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.

- **Key Management function**: The Key Management function includes two sub-functions: Key Request function and Key Delivery function.
- **Key Request function**: The sub-function is responsible for retrieving GBA keys from the BSF, deriving MUK and MRK from GBA keys, performing MBMS User Service Registration, Deregistration and MSK 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 procedures:
  - Bootstrapping initiation
  - Bootstrapping re-negotiation
  - HTTP digest authentication
  - MRK derivation
  - MBMS User Service Registration procedure
  - MBMS User Service Deregistration procedure
  - 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**: The sub-function is responsible for session and transmission functions cf. TS 26.346 [13]. As part of these session and transmission functions, 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 register, 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. The MGV-F is implemented in a protected execution environment to prevent leakage of security sensitive information such as MBMS keys. MGV-S stores the MBMS 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.

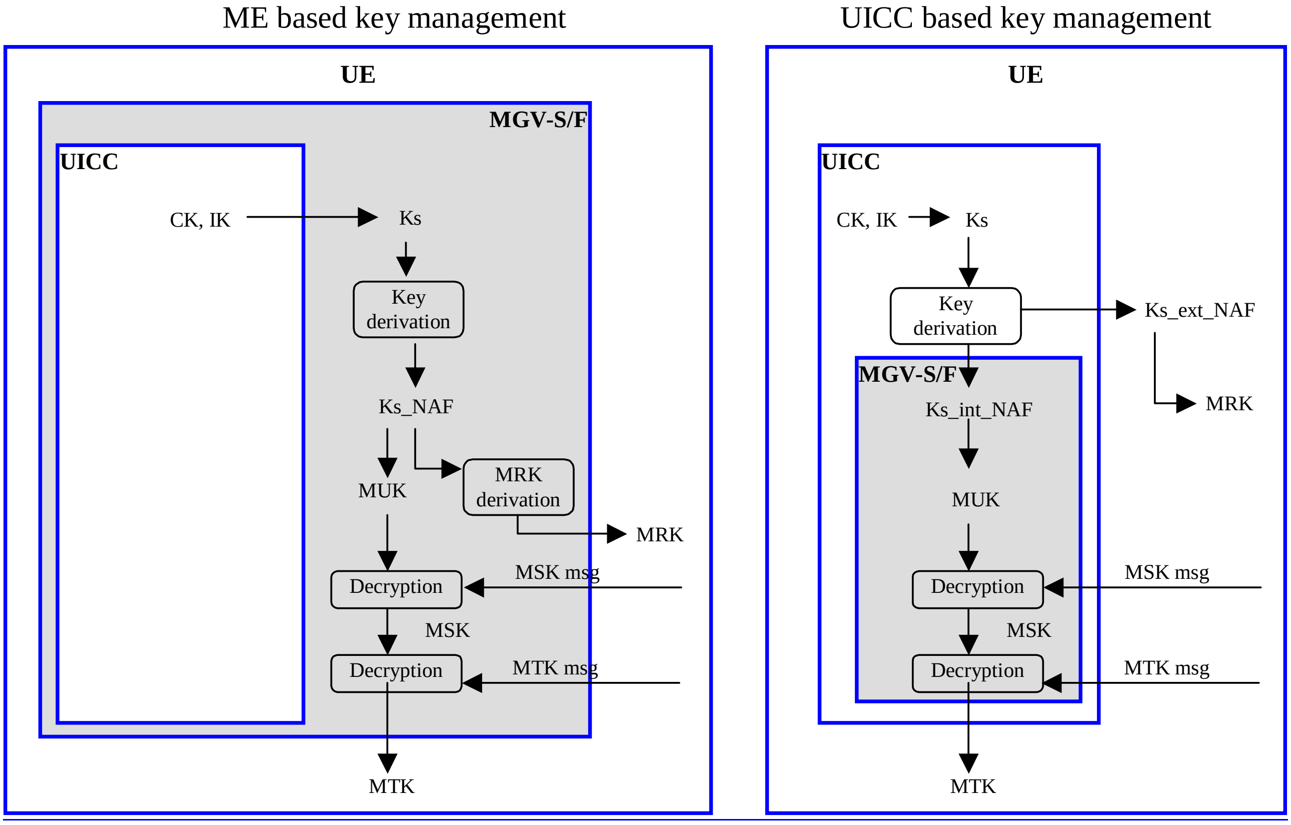


Figure 4.y: ME and UICC based key management in UE

****** 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. The usage of MSKs and MTKs for one Key group is depicted in figure 4.x.

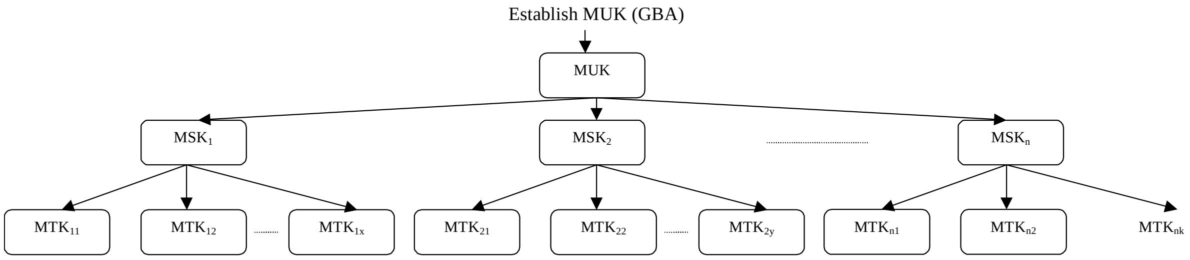


Figure 4.x: MBMS key hierarchy

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

A UE 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 the BM-SC is used to verify the subscription information~~;~~

The following procedures use HTTP digest authentication:

- MBMS User Service Registration procedure (clause 6.3.2)
- MBMS User Service Deregistration procedure (clause 6.3.2)
- MSK request procedure. This can have many triggers (clause 6.3.2)
- 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, it is authenticated as defined in 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:

- MRK derivation (clause 6.1)
- MBMS User Service Registration procedure (clause 6.3.2)
- MBMS User Service Deregistration procedure (clause 6.3.2)
- MSK request procedure (clause 6.3.2)
- MSK delivery procedure (clause 6.3.2)
- MTK delivery procedure (clause 6.3.3)
- BM-SC solicited pull (clause 6.3.2)

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)