

Source: Ericsson
Title: Details of HTTP procedures
Agenda item: MBMS
Document for: Discussion/Decision

1 Introduction

SA3 sent an LS [1] to SA4 and CN1 where it was proposed that the details of MBMS security related HTTP procedures should be specified between SA3 and SA4 and that CN1 TS 24.109 [2] would not specify MBMS security procedures. This contribution describes how the MBMS security related HTTP procedures could be implemented in the specifications.

2 Discussion

MBMS security is related to the following HTTP procedures:

- Bootstrapping procedures (including bootstrapping, initiation and re-negotiation)
- HTTP digest authentication (this is used to protect the MSK request and Associated delivery procedures)
- MSK request procedures (this can have several triggers, e.g. service announcement, missed key update, BM-SC solicited pull)
- Associated delivery procedures in SA4 TS 26.346 use HTTP

Bootstrapping as such is independent of MBMS application. The stage 3 details of bootstrapping procedures are described TS 24.109. For bootstrapping it is proposed to refer to TS 33.220 [3] for stage 2 and to TS 24.109 for stage 3 description. Bootstrapping initiation and re-negotiation are application specific Ua interface procedures. It is proposed that stage 2 of bootstrapping initiation and re-negotiation are specified in TS 33.246 [4] and that TS 24.109 is referred for stage 3 description. Even though TS 24.109 does not explicitly mention MBMS security, it should be possible to refer to that TS from TS 33.246.

HTTP digest authentication can be applied to any HTTP interaction. The stage 3 details of HTTP digest authentication procedures are described TS 24.109 in a way that is independent of the purpose of the HTTP procedure. It is proposed that stage 2 of HTTP digest authentication is specified in TS 33.246 and that TS 24.109 is referred for stage 3 description.

The stage 3 details of MSK request procedures are not currently specified anywhere. It is proposed that the exact message format of HTTP messages and an example signalling flow are specified as annexes in TS 33.246.

The associated delivery procedures are specified in TS 26.346 [5]. It is seen sufficient that TS 33.246 specifies that HTTP digest authentication is used to protect these procedures.

It is also proposed that MBMS specific HTTP error procedures are specified as annex in TS 33.246.

In addition to the HTTP procedures, the exact format of security parameters in service description and the format of HTTP payload for MSK request need to be specified. SA4 TS 26.346 already has placeholders for the security parameters in service description, therefore it is natural that SA4 specifies them. Since SA4 uses XML to define the service description and since both the security parameters in service description and the HTTP payload for MSK request include a list of MSK IDs, it is proposed that SA4 TS specifies the HTTP payload as XML schema. This XML schema should be registered in IANA as a vendor specific MIME type, for example as "[application/vnd.3gpp.mbms-msk+xml](#)". This follows the approach how B-TID and lifetime are specified for Ub interface in TS 24.109.

3 Conclusion & Proposal

This contribution has proposed how MBMS security related HTTP procedures are handled in the specifications. The proposal is implemented in TS 33.246 with the accompanying CR.

4 References

- [1] S3-040884, "LS on MBMS security finalisation", SA3
- [2] TS 24.109, "Bootstrapping interface Ub and Network application function interface Ua"
- [3] TS 33.220, "Generic Bootstrapping Architecture"
- [4] TS 33.246, "Security of MBMS"
- [5] TS 26.346, "MBMS Protocols and codecs"

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

Tdoc **Att_S3-050081**

CR-Form-v7.1
CHANGE REQUEST
⌘ 33.246 CR 044 ⌘ 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:	⌘ Clarification of HTTP procedures		
Source:	⌘ Ericsson		
Work item code:	⌘ MBMS	Date:	⌘ 14/2/2005
Category:	⌘ C	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Use <u>one</u> 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. 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, 6.2.1.1-6.2.1.1.4 (new), 6.3, 6.3.2.2.1, Annex F (new), Annex G (new)								
Other specs Affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;">Y</td> <td style="text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">Y</td> <td style="text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">N</td> <td style="text-align: center;">N</td> </tr> </table> Other core specifications Test specifications O&M Specifications	Y	N	Y	N	N	N	⌘ TS 26.346	
Y	N								
Y	N								
N	N								
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"](#).

***** 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 ~~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 Initiation of bootstrapping

If the UE sends an HTTP request to the BM-SC without any GBA related parameters, the BM-SC replies with HTTP 401 Unauthorized message that requires UE to initiate bootstrapping over Ub interface by indicating 3GPP-bootstrapping in the realm attribute. The details of the form of HTTP 401 Unauthorized message are specified in clause 5.2 of [xx].

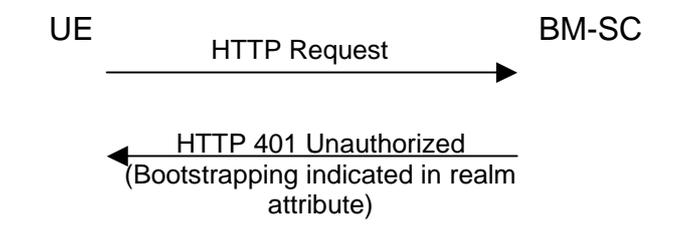


Figure X.X: Bootstrapping initiation

6.2.1.3 Bootstrapping

The Bootstrapping shall follow the procedures as specified in [6] and details are specified in clause 4 of [xx].

6.2.1.4 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 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~~ if client payload is present in the of HTTP Digest message, it shall be integrity protected.

~~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.~~

6.2.1.5 Bootstrapping re-negotiation

If the BM-SC requires an update of the GBA keys when the UE sends an HTTP request message, the BM-SC replies with HTTP 401 Unauthorized message that requires the UE to initiate bootstrapping over Ub interface as in clause

[6.2.1.2 but with the message protected by the current MRK. The details of the form of this message are specified in clause 5.2 of \[xx\].](#)

******* 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.

******* 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.

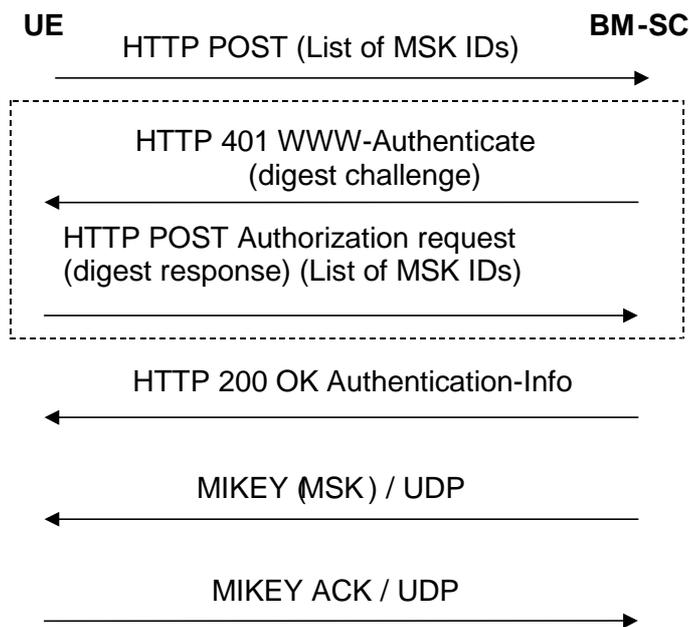


Figure 6.1: Basic MSK retrieval procedure

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.

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.

The details of the HTTP messages 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].

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 MSK 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 be based on GBA and more generally on the HTTP Digest authentication as described in clause 6.2 of the present document.

F.2 MSK request procedure

The MSK request procedure contains the following request. The same procedure is used to initiate the MSK key management and to request the MSKs the UE may require:

- an MSK request in the form XML document, see TS 26.346;

The request is followed by a response from the BM-SC indicating success or failure

F.2.1 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 [14];
- 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", depending on the UE's desired request type (e.g. Request-URI may take the form of " [/bmsc.home1.net/keymanagement?requesttype=msk-request](http://bmsc.home1.net/keymanagement?requesttype=msk-request)" for MSK request delivery);
- the UE may add additional URI parameters to the Request-URI;
- the HTTP header Content-Type shall be "application/vnd.3gpp.mbms-msk+xml ". The XML schema of payload is specified in [13];

Editor's Note: The MIME type name should be confirmed with SA4

- 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 shall verify that the subscriber is authorized to receive the particular MSK by checking the subscriber's subscription and possibly user security settings received from the BSF as specified 3GPP TS 33.220 [4].

Editor's Note: Subscriber's user security setting for BM-SC are FFS.

Upon successful subscriber subscription 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.2.2 Error situations

MSK request 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 [14]. 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 MSK retrieval and their mappings to HTTP Status Codes are described in table F.2.2-1.

NOTE: In table F.2.2-1, the "Description" column describes the error situation in BM-SC. The "BM-SC error" column describes the typical reason for the error.

Table F.2.2-1: HTTP Status Codes used for MSK request error

<u>HTTP Status Code</u>	<u>HTTP Error</u>	<u>UE should repeat the request</u>	<u>Description</u>	<u>BM-SC error</u>
<u>400</u>	<u>Bad Request</u>	<u>No</u>	<u>Request could not be understood</u>	<u>Request was missing, or malformed</u>

<u>HTTP Status Code</u>	<u>HTTP Error</u>	<u>UE should repeat the request</u>	<u>Description</u>	<u>BM-SC error</u>
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	MSK request was valid, but subscriber is not allowed to retrieve this particular MSK or MSK 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 MSK management procedure.

G.2 Introduction

G.2.1 General

BM-SC and UE use keys derived from GBA keys to authenticate and integrity protect the HTTP communications.

G.3 Signalling flows demonstrating a successful MSK request procedure

G.3.1 Successful MSK request procedure

The signalling flow in figure G.3.1-1 describes the message exchange between UE and BM-SC when UE wants to request MSK.

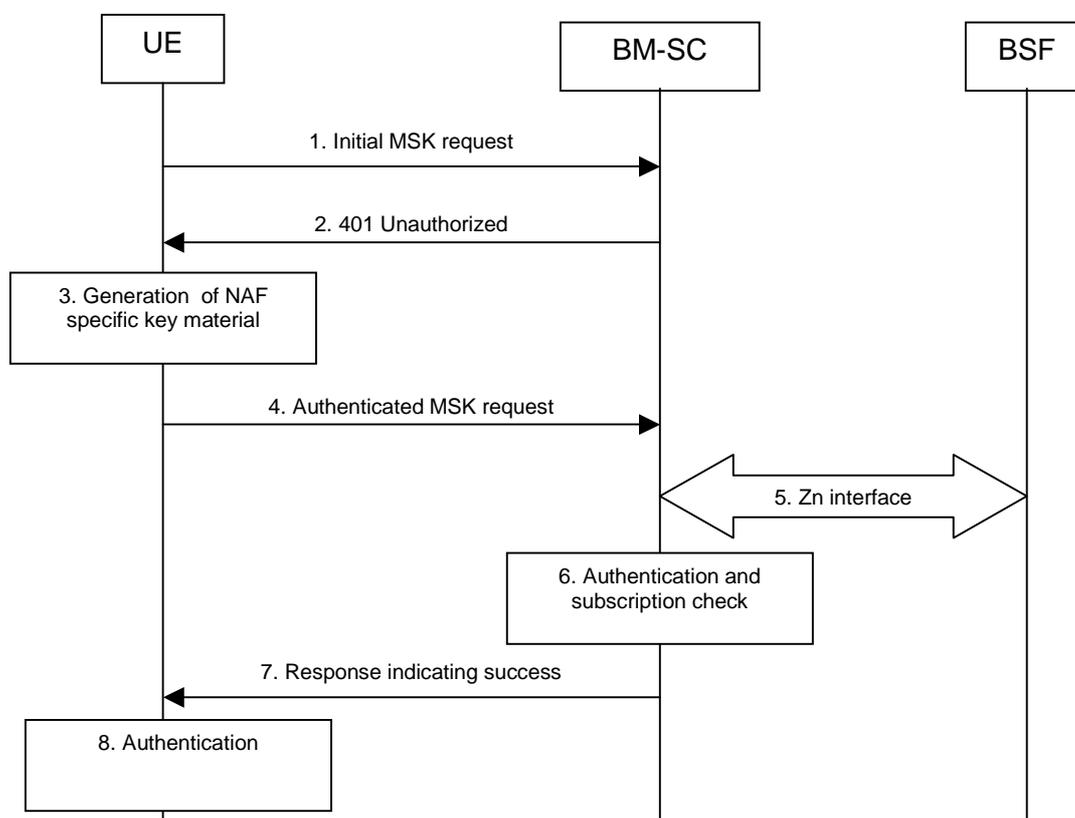


Figure G.3.1-1: Successful subscriber certificate enrolment.

1. Initial MSK request (UE to BM-SC) - see example in table G.3.1-1

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

Table G.3.1-1: Initial MSK request (UE to BM-SC)

```
POST /bmsc.homel.net/keymanagement?requesttype=msk-request HTTP/1.1
Host: bmsc.homel.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.homel.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.

Editor's Note: The MIME type needs to be specified in SA4 TS 26.346.

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 will 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.3.1-2

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.3.1-2: 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.homel.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 K_s NAF 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.3.1-3

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 NAF specific key material K_s NAF (base64 encoded) as the password, and sends the request to BM-SC.

Table G.3.1-3: Authenticated enrolment request (UE to BM-SC)

```
POST /bmsc.homel.net/keymanagement?requesttype=msk-request HTTP/1.1
Host: bmsc.homel.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.homel.net:1234/service
Authorization: Digest username="(B-TID)", realm="3GPP-bootstrapping@bmsc.homel.net",
nonce="a6332ffd2d234==", uri="/bmsc.homel.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 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 (K_s NAF) and subscriber's user security setting from the BSF. BM-SC further derives MBMS specific key material MRK and MUK as specified in clause 6.1.

Editor's Note: Subscriber's user security setting for BM-SC are FFS.

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

Table E.3.1-4: Bootstrapping authentication information procedure (BM-SC to BSF)

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

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 material Ks_NAF obtained from BSF. BM-SC calculates the corresponding digest values using Ks_NAF, 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 subscription data within the BM-SC and subscriber's user security setting received from the BSF in step 5.

7. Response indicating success (BM-SC to UE) - see example in table G.3.1-5

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 key material Ks_NAF 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 E.3.1-5: Delivery of subscriber certificate (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.