3GPP TSG SA WG3 Security — S3#32 **S3-040058**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda Item: MBMS
Source: Ericsson

Title: Usage of GBA, MIKEY and HTTP digest for MBMS key delivery

Document for: Discussion/Decision

1. Introduction

In SA3#31 Munich meeting the MBMS key management was discussed and it was decided that:

"For the ME part, GBA and MIKEY (with possible 3GPP-specific enhancements, e.g. for the support of encrypted keys) will be used as a basis for the standardised solution. This does not rule out DRM based solutions, e.g. DOWNLOAD".

SA3 decided also on two-tiered key management solution, where the 'high level' MBMS key is delivered to the UE with point-to-point and the 'low level' MBMS key is delivered with point-to-multipoint manner. This contribution discusses how the high level MBMS key is delivered to the UE and does not restrict how the high and low level MBMS keys are used eventually in MBMS data protection. Thus the solution is applicable to MBMS key management solutions in general.

This contribution explores how GBA and HTTP digest can be used with MBMS. The contribution intends to identify open issues on the usage of GBA in MBMS.

2. Usage of GBA in MBMS

2.1 GBA in MBMS

The following discusses GBA in MBMS and identifies open issues.

This contribution assumes that HTTP digest and MIKEY are used in MBMS. Note that this has not been agreed in SA3.

HTTP digest [1] is used between UE and NAF (i.e. BM-SC). Using HTTP digest provides mutual authentication and integrity protection for MBMS key request and key delivery messages. The transaction identifier from GBA is used as username and the Ks as the password.

MIKEY [2] is used for encrypted key delivery. It should be noted that MIKEY has functionality to generate the KEK from the bootstrapped key material. The KEK generation with MIKEY can be regarded to consist of two parts: First, the GBA procedure is used between UE and BSF to provide the pre-shared key material to the UE and BSF. This procedure is used as is described in GBA TS 33.220 [3] chapter 4.3.2. Second, when the UE accesses the NAF (i.e. BM-SC) using the HTTP digest procedure, MIKEY implementations in UE and NAF generate the KEK from the pre-shared key material.

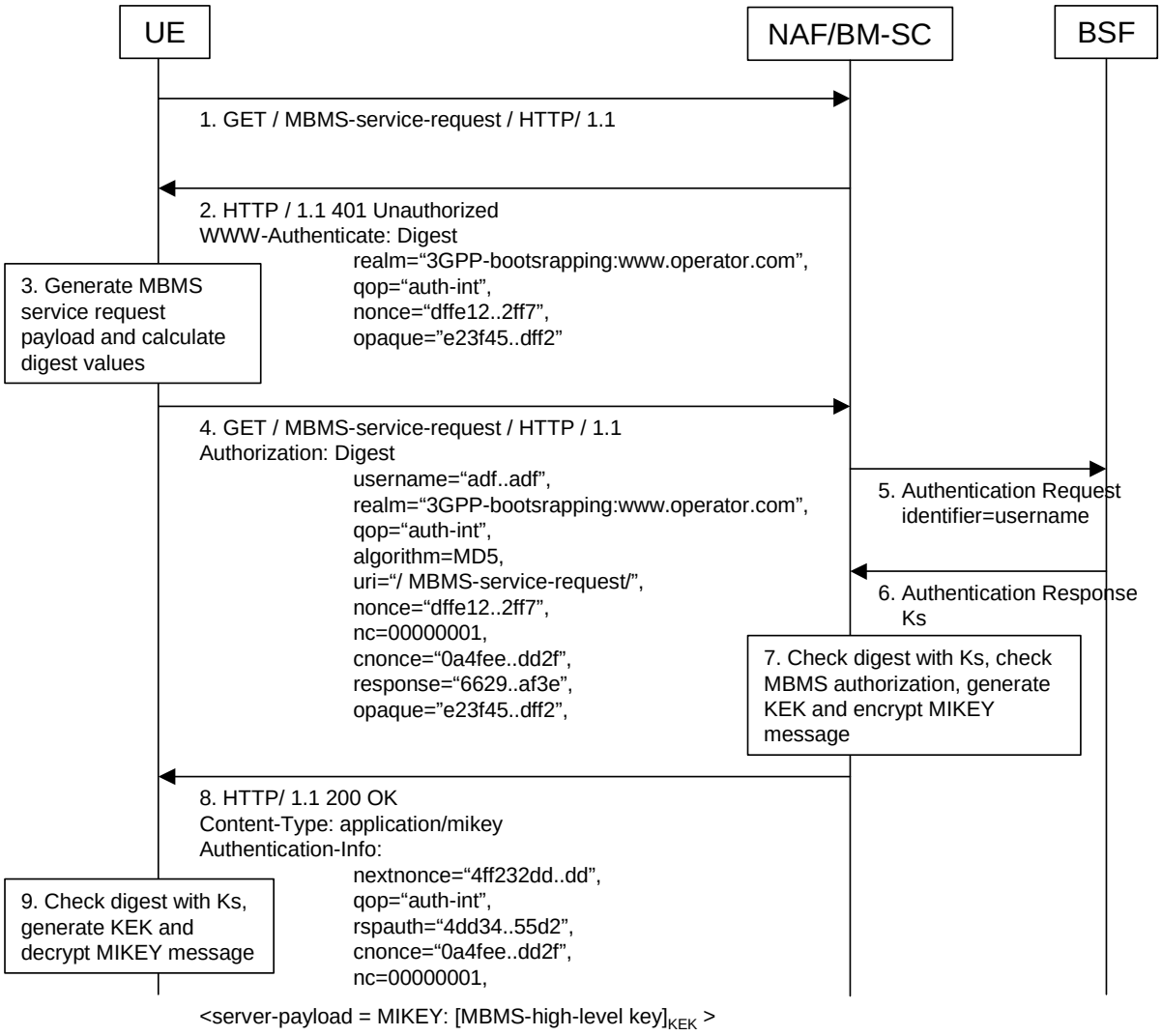

Figure 1 Usage of GBA in MBMS

The overview of HTTP digest usage for MBMS is depicted in figure 1. It is based on Annex A in TS 33.220.

1. UE sends an HTTP GET request to NAF in order to request for a specific MBMS service, see open issue1 in 2.2.

2. NAF responds with HTTP 401 Unauthorized, which contains the WWW-Authenticate header and HTTP digest challenge.

3. The UE generates the HTTP request for the MBMS service and calculates the Authorization header values using the transaction identifier it received from the BSF as username and the session key Ks as the password.
   See open issue 2.

4. UE sends the HTTP request to NAF to request for specific MBMS service.

5. NAF requests the session key Ks from the BSF using the transaction identifier.

6. BSF responds to the NAF with the session key Ks.
   See open issue 3.

7. NAF verifies the Authorization header values using the transaction identifier it received from the BSF as username and the session key Ks as the password. NAF verifies that the UE is authorized to access the requested MBMS service.

NAF generates the KEK using Ks as key material. *See open issue 4.*
NAF generates the MIKEY message including the high level MBMS key and protects it with the KEK.

8. NAF generates the HTTP 200 OK message. Authentication-Info header values are calculated using session key Ks. MIKEY message is included as server payload. The Content-Type indicates the MIME type of the payload to be application/mikey.

9. The UE receives the response and verifies the Authentication-Info header. The UE generates the KEK and integrity key for MIKEY ONLY if this is the first MIKEY message for a specific Ks. The UE decrypts the high level MBMS key from the MIKEY message.

Re-keying

The HTTP digest procedure may be used also for re-keying purpose.

In normal re-keying case it is assumed that Ks has not expired and thus the username has not changed so steps 5 and 6 are not taken. It is also assumed that the NAF has sent the next-nonce value in step 8 in the previous digest procedure. In this case the UE may start the re-keying from step 4 since it may use the next-nonce value and thus the NAF is able to authenticate the Authorization header. NAF will send a new key with step 8.

If the next-nonce value is not used in step 4, the NAF may send a new digest challenge as in step 2. This means an extra round trip compared to the case above.

If the username has changed, see below.

Change of Ks

When the Ks has expired, a new GBA procedure needs to be run resulting in a new transaction identifier and Ks. This means that a new username and password for are used in HTTP digest, respectively.

When the UE accesses the NAF next time for re-keying, it may start from step 4 and send the new username to the NAF. Since the username is unknown to the NAF, it will prompt the UE to authenticate itself with HTTP digest challenge with a fresh nonce as in step 2. The UE will respond with message 4. Using the new username NAF is then able to fetch the new Ks from the BSF. It should be noted that a new Ks will trigger the generation of a new KEK.

Lifetime of KEK

Since the KEK is derived from Ks, the lifetime of KEK is depending on the lifetime of Ks. The KEK is generated only when the Ks is used for the first time. For subsequent key deliveries between BM-SC and UE the KEK remains the same for the lifetime of the Ks.

2.2 Open issues

The following open issues are identified:

1. **Annex A in 33.220 shows that the UE sends an empty message to the NAF in step 1.** However, this is incorrect since the client (UE) should always request for a specific service from the server (NAF). The client is not assumed to know a priori that the server will require digest authentication.

2. **Identifying the requested service**
   This paper assumes that the UE identifies the requested MBMS service in the URI field of the Authorization header, e.g. by a path mbms.operator.com/mbms-service-ID/mbms-session-ID.
   It should be studied whether the URI field is sufficient or if the client payload is needed. The client payload would enable sending more specific service request.
   The client payload might be needed in the case when the UE detects from the key-id that it has not got the current MBMS key and the UE needs to request it from the NAF. In this case it needs to be specified how to carry and protect the client payload (e.g. key-id).
   It is proposed to make a working assumption that the MBMS service is identified with URI and no client payload is included.

It is also proposed to add an editor's note to TS 33.246 [4] that the need for client payload in key request messages should be studied further.

3. **Is UE identifier received from BSF?**
The NAF has no knowledge of which UE is in question unless it receives the UE identifier, e.g. IMSI, from the BSF. This issue is discussed in another paper from Ericsson, cf [5].

4. **Is Ks further derived?**
It is an open issue whether the bootstrapping key material Ks is used as KEK or whether it is further derived before KEK generation? As noted already in section 2.1 MIKEY has functionality to derive KEK from a pre-shared key material.
It is proposed that MIKEY KEK derivation functionality is used to generate the KEK as specified in clause 4.1.4 of MIKEY [2]. The MIKEY KEK generation uses pseudo random (PRF) function, which is specified in clause 4.1.2 of [2]. The KEK derivation function can be defined as:

KEK = PRF (pre-shared key, pre-shared key length, output key length, constant || 0xFF || CSB-id || RAND),

where the constant defines the type of the key to be generated, i.e. encryption key or authentication key, the CSB-id identifies the crypto session bundle (CSB) that can be used to identify the MBMS service, and RAND, which is received in the first MIKEY message from the BM-SC to the UE.

Since the CSB-id is part of the KEK generation and it also can be used to identify the MBMS service in MIKEY, there will be a KEK per MBMS service in the UE. Re-authentication of the UE will result to new KEK for each MBMS service.

5. **Support for NAF in visited networks in MBMS and GBA in Release 6**
It seems to be unclear whether the NAF (BM-SC) can be in visited network in Release 6. TS 33.220 [3] states in editor's note in Scope and in 4.1.3. the following:

"*Editor's note: The specification objects are scheduled currently in phases. For the first phase of standardisation, only the case is considered where bootstrapping server functionality and network application function are located in the same network as the HSS. In later phases, other configurations may be considered.*"

But at the same time it is stated in TS 33.220 in requirements section 4.1:
"*The architecture shall not preclude the support of network application function in the visited network, or possibly even in a third network*"

TS 33.246 [4] states in 5.1:
Editor's note: The use of AKA between the BM-SC and UE was proposed. It was concluded that the issue of bootstrapping and having the BM-SC in the visited network need to be further investigated

The support for NAF in visited networks in MBMS in release 6 should be clarified.
It is proposed that NAF is allowed to be in visited network in MBMS in release 6, but the BSF will reside in home network. However, if BSF and NAF are in different networks, this might require two PDP contexts in the UE. Therefore it is proposed that SA3 sends an LS to SA2 to inquire further information whether SA2 sees problems in having the BSF and NAF in different networks.

3. Proposal

It is proposed that the procedure described in this contribution is taken as a basis for further development of GBA usage in MBMS. It is also proposed that SA3 takes the proposed working assumptions.

4. References

[1] RFC 2617, HTTP Authentication: Basic and Digest Access Authentication

[2] MIKEY: Multimedia Internet KEYing, IETF Internet Draft, <draft-ietf-msec-mikey-08.txt>, December, 2003

[3] TS 33.220, Generic Bootstrapping Architecture, v 1.0.0

[4] TS 33.246, Security of Multimedia Broadcast/Multicast Service, v 1.0.0

[5] TD-S3-040xxx, Requirements for transaction identifier in GBA, SA2#32, Ericsson