3GPP TSG SA WG3 Security — S3#32 **S3-040057**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda Item: MBMS
Source: Ericsson

Title: ~~Usage of GBA, MIKEY and HTTP digest for MBMS key delivery~~Status of SRTP and MIKEY in IETF

Document for: Information~~Discussion/Decision~~

1. Introduction

This contribution informs SA3 about the status of SRTP [1] and MIKEY [2] protocols in IETF.

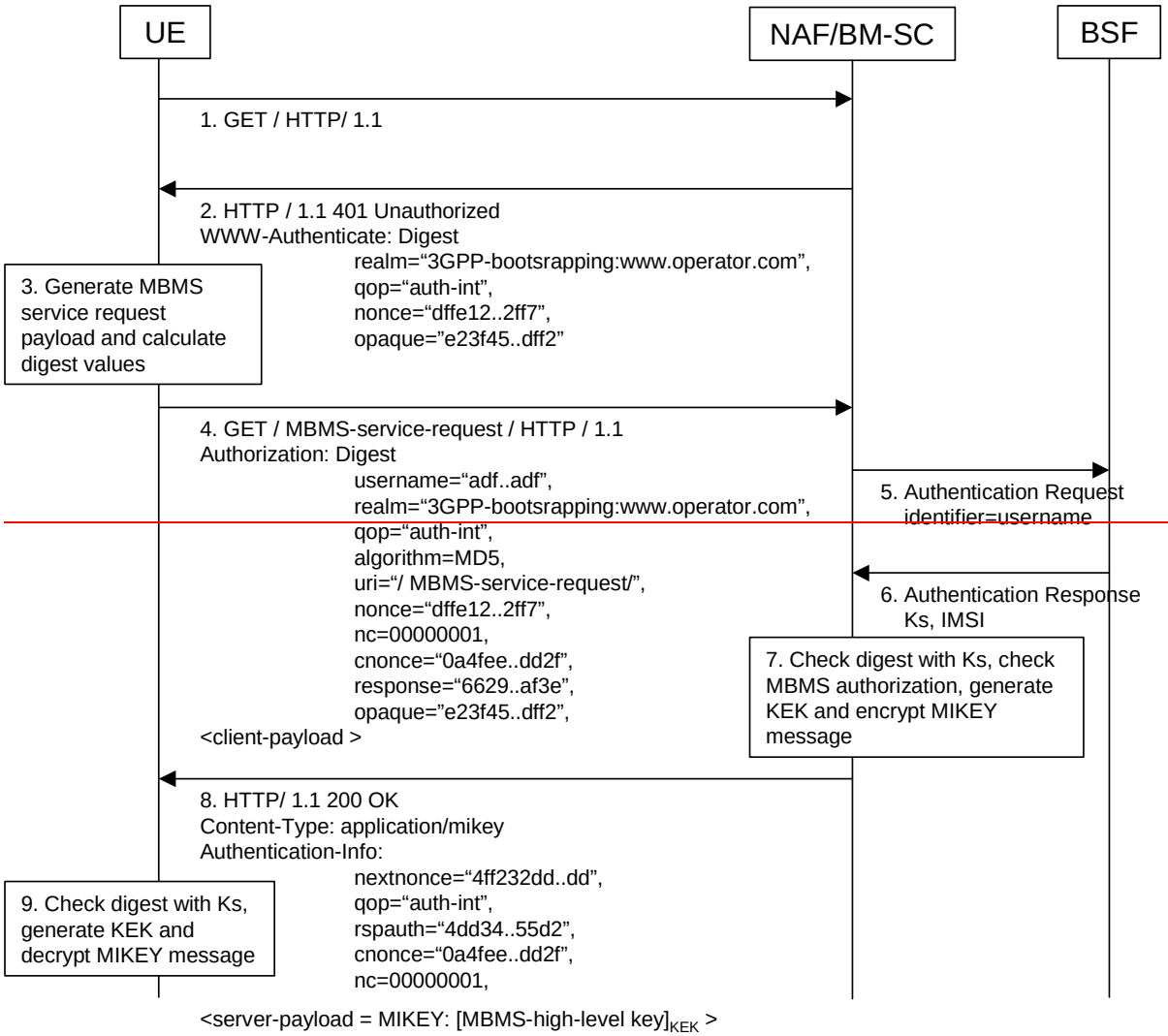
~~In SA3#31 Munich meeting the MBMS key management was discussed and it was decided that:~~

~~*"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".*~~

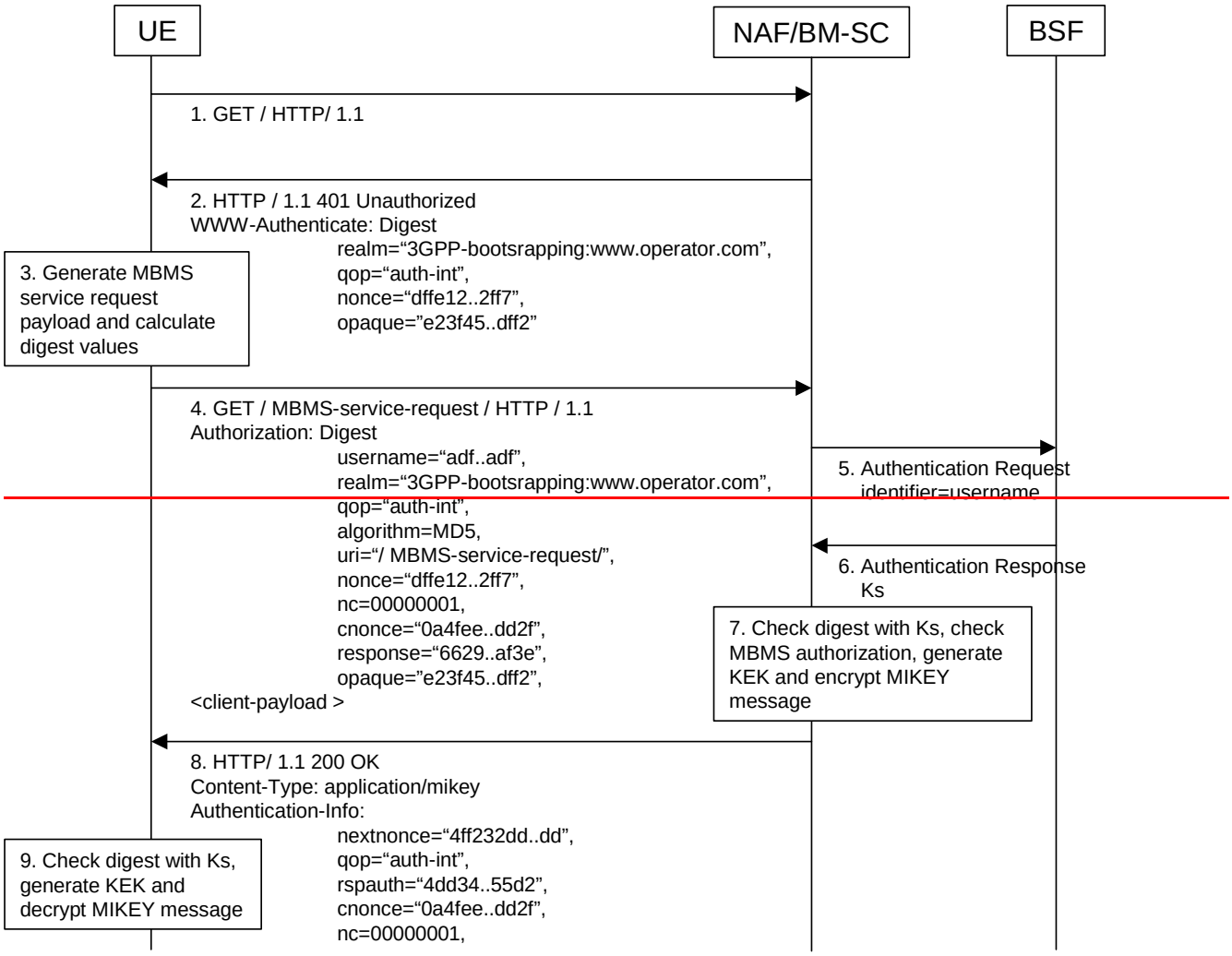
~~This contribution explores how GBA can be used to generate key encryption key (KEK) for MBMS key delivery with MIKEY. It is also described how MIKEY is used as key management protocol and HTTP digest for integrity protection of MBMS key delivery mechanism.~~

2. Status of SRTP

SRTP (Secure Real-time Transport Protocol) has been approved by IESG and has received RFC status although an RFC number has not been assigned to it
yet.


UE
NAF/BM-SC
BSF
1. GET / HTTP/ 1.1
2. HTTP / 1.1 401 Unauthorized
WWW-Authenticate: Digest
realm="3GPP-bootsrapping:www.operator.com",
qop="auth-int",
nonce="dffe12..2ff7",
opaque="e23f45..dff2"
3. Generate MBMS service request payload and calculate digest values
4. GET / MBMS-service-request / HTTP / 1.1
Authorization: Digest
username="adf..adf",
realm="3GPP-bootsrapping:www.operator.com",
qop="auth-int",
algorithm=MD5,
uri="/ MBMS-service-request/",
nonce="dffe12..2ff7",
nc=00000001,
cnonce="0a4fee..dd2f",
response="6629..af3e",
opaque="e23f45..dff2",
<client-payload >
5. Authentication Request
identifier=username
6. Authentication Response
Ks, IMSI
7. Check digest with Ks, check MBMS authorization, generate KEK and encrypt MIKEY message
8. HTTP/ 1.1 200 OK
Content-Type: application/mikey
Authentication-Info:
nextnonce="4ff232dd..dd",
qop="auth-int",
rspauth="4dd34..55d2",
cnonce="0a4fee..dd2f",
nc=00000001,
9. Check digest with Ks, generate KEK and decrypt MIKEY message
<server-payload = MIKEY: [MBMS-high-level key]KEK >

~~Usage of GBA~~



~~A key encryption key (KEK) is needed to protect the point-to-point key delivery from the BM-SC to the UE. MIKEY itself can be used for KEK generation since the MIKEY specification [xxx] defines functionality for generating KEK (and also integrity key) from a pre-shared key material.~~

~~The KEK generation for 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 chapter 4.3.2. Second, when the UE accesses the NAF (i.e. BM-SC), MIKEY implementations in UE and NAF generate the KEK (and integrity key) from the pre-shared key.~~

~~How to receive/ generate the KEK in UICC based solution?~~

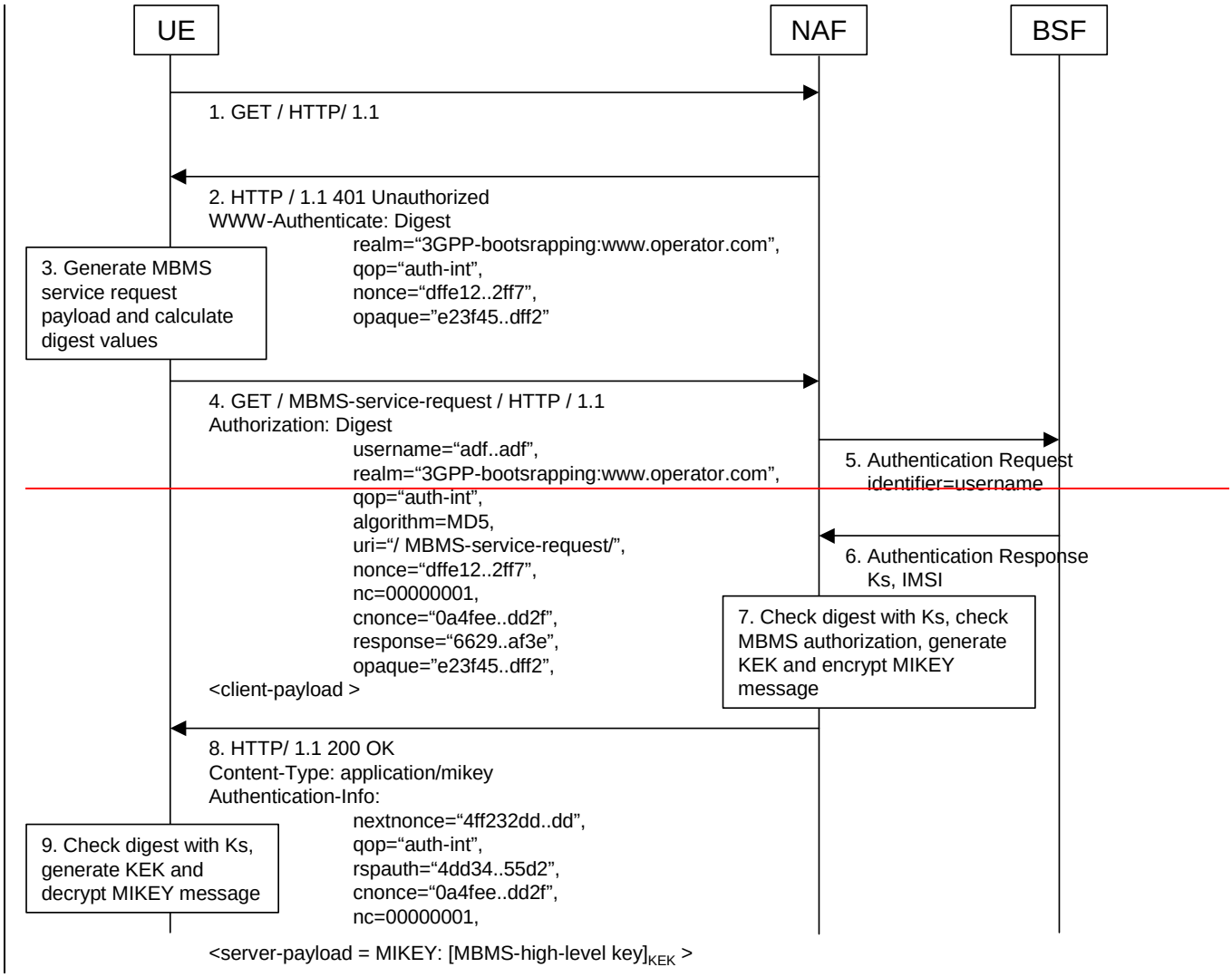
~~3.Usage of HTTP digest and MIKEY for MBMS key delivery~~

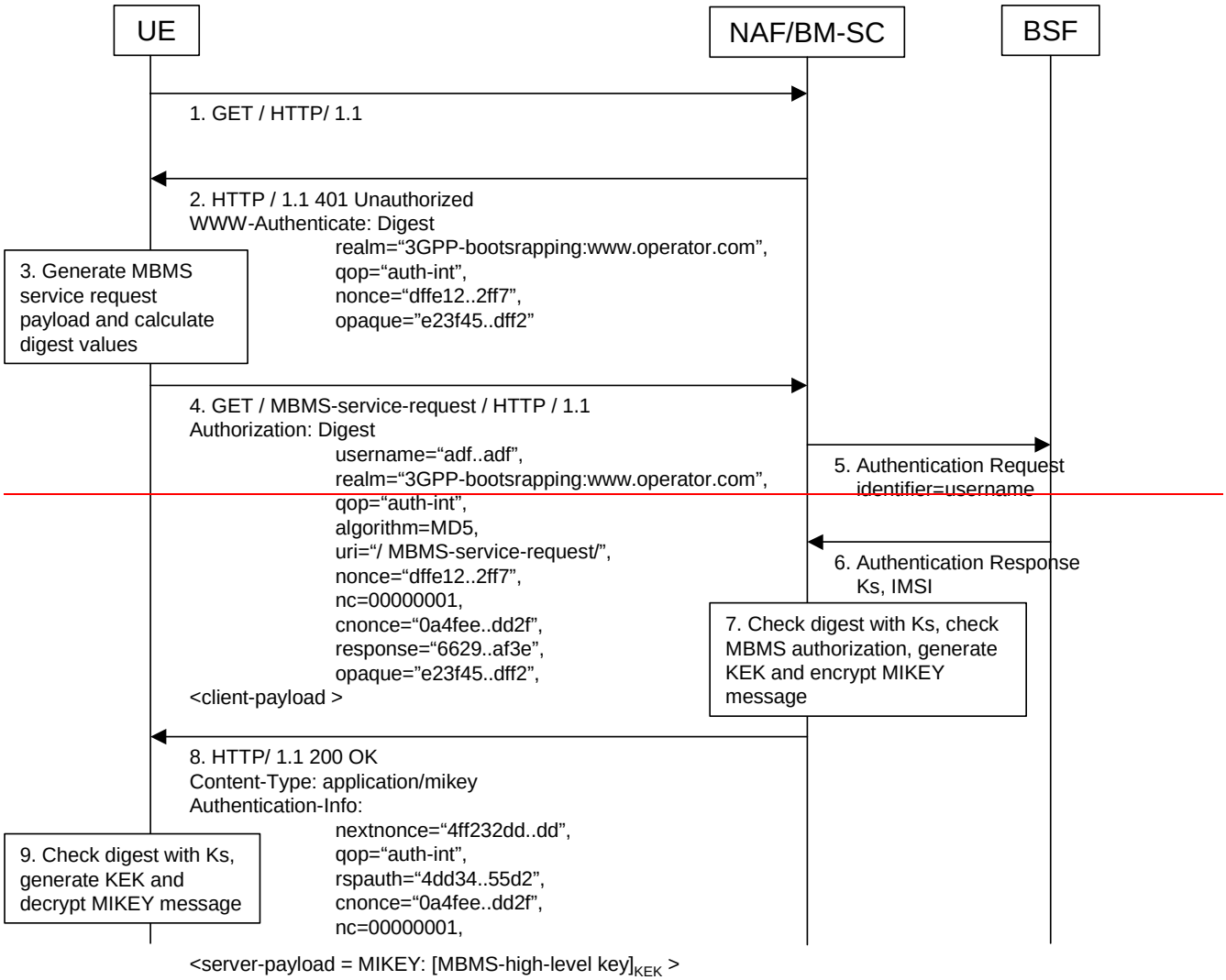
~~The following describes how HTTP digest and MIKEY are used for MBMS key delivery. It also shows how the bootstrapped key material is used in KEK generation. The transaction identifier from GBA is used as username and the Ks as the password.~~

~~SA3 has decided earlier 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 solution~~

~~describes 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.~~

~~3.1 Overview of HTTP digest for MBMS key delivery~~


UE
NAF
BSF
1. GET / HTTP/ 1.1
2. HTTP / 1.1 401 Unauthorized
WWW-Authenticate: Digest
realm="3GPP-bootsrapping:www.operator.com",
qop="auth-int",
nonce="dffe12..2ff7",
opaque="e23f45..dff2"
3. Generate MBMS service request payload and calculate digest values
4. GET / MBMS-service-request / HTTP / 1.1
Authorization: Digest
username="adf..adf",
realm="3GPP-bootsrapping:www.operator.com",
qop="auth-int",
algorithm=MD5,
uri="/ MBMS-service-request/",
nonce="dffe12..2ff7",
nc=00000001,
cnonce="0a4fee..dd2f",
response="6629..af3e",
opaque="e23f45..dff2",
<client-payload >
5. Authentication Request
identifier=username
6. Authentication Response
Ks, IMSI
7. Check digest with Ks, check MBMS authorization, generate KEK and encrypt MIKEY message
8. HTTP/ 1.1 200 OK
Content-Type: application/mikey
Authentication-Info:
nextnonce="4ff232dd..dd",
qop="auth-int",
rspauth="4dd34..55d2",
cnonce="0a4fee..dd2f",
nc=00000001,
9. Check digest with Ks, generate KEK and decrypt MIKEY message
<server-payload = MIKEY: [MBMS-high-level key]KEK >



~~The overview of HTTP digest usage for MBMS is depicted in figure x. It should be noted that some details are omitted for simplicity. Some specific issues are discussed in section 3.2.~~

~~1.UE sends an empty HTTP GET request to NAF in order to trigger communication with NAF.~~

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

~~3.The UE generates client-payload containing the MBMS service request that it wants to send to NAF. Then it will generate the HTTP request by calculating the Authorization header values using the transaction identifier it received from the BSF as username and the session key Ks as the password.~~

~~4.UE sends the HTTP request to NAF to request for specific MBMS service.~~
~~NOTE: It is FFS, if some kind of MBMS service request is in the client payload and how it would be carried in HTTP. A simpler alternative could be to indicate the requested MBMS service in the URI field, for example mbms.operator.com/mbms-service-ID/mbms-session-ID.~~

~~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 and UE identifier, e.g. IMSI.~~

~~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. Then NAF verifies that the UE is authorized to access the requested MBMS service. NOTE: It is FFS, where NAF gets this authorization information. Then~~

NAF generates the KEK and integrity key using Ks as key material and using functionality specified in MIKEY. Then NAF generates the MIKEY message including the high level MBMS key and protects it with the KEK and the integrity key.

8.NAF generates the HTTP 200 OK message. Authentication Info header is included using session key Ks to integrity protection and authentication. MIKEY message is put 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. Then the UE authenticates the MIKEY message and decrypts the high level MBMS key from the MIKEY message.

3.2 Discussion

Some specific notions can be done on the solution.

Authentication

Using HTTP digest provides mutual authentication and integrity protection for MBMS key request and key delivery messages. The MIKEY message carried inside HTTP is integrity protected and the key material part of the message is encrypted.

Identifying the requested service

The UE identifies the requested MBMS service in step 4 above. It might be possible to identify the MBMS service in the URI field of the Authorization header, e.g. by a path mbms.operator.com/mbms-service-ID/mbms-session-ID. A typical use case could be that a user activates the service on the operator's web pages.

The service could be identified also in the client payload or the client payload could be used in addition to the URI if more information is needed in the service request. This would enable sending more specific service request, for example a request to send more than one MBMS keys at a time to the UE. This is FFS.

These alternatives could be phased so that URI is used in the first phase and client payload in later phases.

The client payload might be needed anyway 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. (How to convey key-id with integrity protection? Is there an existing MIME type?)

Re-keying

The UE may use the HTTP digest procedure also for re-keying purposes. The UE may start immediately from step 4 since it may use the next-nonce value that was received from the NAF in the previous digest operation in step 8. If the UE does not use the next-nonce value, it has to start from step 1.

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. It should be noted that this means that KEK lifetime is independent of the lifetime of the high level MBMS key.

Lifetime of Ks

The lifetime of Ks is FFS. However, 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 (to request for a new service or for re-keying), it may start from step 4 and send the new username to the NAF (another alternative is to start from step 1). Since the username is unknown to the NAF, it will prompt the UE with HTTP digest challenge as in step 2. Eventually the NAF is able to associate the username to the UE when the NAF has communicated with the BSF in steps 5 and 6. A new Ks will trigger the generation of a new KEK.

3. Status of MIKEY

~~4.~~MIKEY (Multimedia Internet KEYing) has been approved by IESG and has received RFC status although an RFC number has not been assigned to it yet.

The document includes also a MIME type definition for MIKEY. Thus it can be carried, e.g. over HTTP.~~Proposal~~

~~MIKEY specification [xxx] defines functionality for generating KEK (and also integrity key) from a pre-shared key material. For ME based solution it is proposed that MIKEY key generation functionality is used to generate the KEK from the GBA key material (Ks). It is also proposed that HTTP digest with MIKEY is used for key delivery in MBMS.~~

~~5.Conclusion~~

~~6.~~4. References

[1] The Secure Real-time Transport Protocol, IETF Internet Draft, <draft-ietf-avt-srtp-09.txt>, July 2003

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