3GPP TSG SA WG3 Security — S3#36 **S3-041012**

Shenzhen, China, November 23-26, 2004

Source: **Siemens**

Title: **MUK ID**

Document for: **Discussion and Decision**

Agenda Item: **MBMS**

1 Introduction

The contribution analyses the possibilities to identify the key MUK which is shared between a particular BM-SC and a particular UE. The MUK identification is necessary for the outer Key ID of a ptp MIKEY message to transfer an MSK from a BM-SC to the UE (TS 33.246 clause 6.4.4 General Extension Payload). MSK-ID and MTK-ID are respectively restricted to two bytes. It is analyzed if this is also possible for the MUK-ID.

2 NAF-ID based MUK Identification

According to TS 33.246 the key MUK is an MBMS user individual key that is used by the BM-SC to protect the point to point transfer of MSK's to the UE. This key is derived from the Ks_NAF (in case of ME based key management) or from Ks_int_NAF (in case of UICC based key management). The Key MRK has similar properties as MUK, but is exclusively used by the ME within http requests, while the key MUK is used in the reverse direction within the MIKEY protocol.

A UE may have joined different MBMS services at the same time which may be hosted by different BM-SC of different operator networks. A BM-SC can be identified uniquely by a NAF-ID and while there should be –in principle- only one MUK in use per {BM-SC, UE} pair at a certain moment, is seems obvious to use NAF-ID as a unique MUK identifier.

But is the NAF-ID sufficient to unambiguously identify the right MUK? Let us investigate following scenario: *The BM-SC sends a MIKEY message (first message in a push solicited pull message) using the last valid MUK and a recent GBA bootstrapping has been run which is unknown by the BM-SC.*

The MUK key table (inside the secure storage) could have following status with respect to the MUK

(1) the key with MUK-ID= NAF-ID has expired lifetime but is still available.

(2) the key with MUK-ID= NAF-ID cannot be found

(3) the key with MUK-ID= NAF-ID can be found and has not expired. BUT that MUK is based on a recent GBA-Run, which is unknown to the BM-SC (e.g. a very recent NAF key generation from which the http session was not able to complete towards the BM-SC, and the NAF-key was not removed from the NAF-key list either).

(4) The key with MUK-ID = NAF-ID can be found and is the same as used by the BM-SC.

Evaluation:

(1) the MUK key can be taken from the MUK key table as an exception and the UE can be informed that the MIKEY push solicited pull message was valid. (See also other Siemens MBMS contribution to this meeting).

(2a) the ME decides to generate the MUK first (based on the last TID and NAF-ID) as it cannot find an MUK-ID related to the outer key ID of the received MIKEY message. Now a different MUK will be generated than used by the BM-SC causing a push solicited pull MIKEY message which is silently discarded at the UE[1] due to the inability to authenticate the MIKEY packet.

(2b) alternatively to case 2a the MUK key could be generated automatically by the UICC based on the last GBA-run. *(this would be a possible optimization of the procedures where the ME does not need to call first a NAF key generation procedure)* Similar as with case 2a this would lead to an error in the MIKEY packet authentication.

(3) The same behaviour applies as for case 2a.

(4) No problems.

Conclusion: **The MUK cannot be identified by only using the NAF-ID.**

Within the next section some proposals for MUK-ID are evaluated.

3 Proposals for MUK Identification

A) Extend the NAF-ID based MUK identification to take into account the bootstrapping identification.

1. From TS 33.220 Section 4.5.2 we know that '*The B-TID value shall be also generated in format of NAI by taking the base64 encoded [12] RAND value from step 3, and the BSF server name, i.e. base64encode(RAND)@BSF_servers_domain_name*'

The B-TID at first GBA-run could be: RAND1@BSF.operator1.com

A B-TID at subsequent GBA-run could be: RAND2@BSF.operator1.com

A MUK may be identified by the B-TID in NAI-format or as B-TID derived NAI e.g. RAND1@BMSC1.operator1.com. This proposal (**Base64encoded(RAND)@NAF-ID**) takes into account that the UE shall be able to distinguish the MUK per BM-SC and per bootstrapping run. That it makes the MUK-ID different in length than the MSK-ID (2 bytes) within the MIKEY-message is not a problem for the MIKEY extension. A consequence however is that the RAND needs to be stored (in addition to the MBMS keys) per user at the BM-SC for the lifetime of the MUK (which is longer than the GBA-lifetime due to the push solicited pull procedure). In the next paragraphs we explore other solutions to look if more efficient BM-SC storage can be obtained.

2. A variant of the above solution for MUK identification is to substitute the RAND into a byte. As the UE is always the first to set-up communication using an MRK for the first time (i.e. using a B-TID within the http request towards a particular BM-SC), it seems logical to do the MUK-ID assignment also by the UE. This will require that this parameter can be transported over Ua-interface within the http request in order to let the BM-SC know the assigned MUK-ID when first using the B-TID. Using a NAI format this would be **UE_assigned@NAF-ID**. Using one byte will limit the amount of managed BM-SC to 128, which could be sufficient. The implementation of the algorithm (e.g. take next free higher number or using a hash plus collision avoidance) for assigning the ID number, would be implementation specific.

---

[1] MIKEY RFC clause 5.1.2. on Error Handling

The error message is formed as: HDR, T, {ERR}, {SP}, [V|SIGNr]

Note that if the failure is due to the **inability to authenticate** the peer, the error message is OPTIONAL, and does not need to be authenticated. It is up to the local policy how to treat this kind of messages. However, if a signed error message in response to a failed authentication is returned this can be used for DoS purposes (against the Responder). Similarly, an unauthenticated error message could be sent to the Initiator in order to fool her to tear down the CSB. It is highly RECOMMENDED that the local policy takes this into consideration. Therefore, in case of authentication failure, one advice would be not to authenticate such an error message, and when receiving an unauthenticated error message only see it as a recommendation of what may have gone wrong.

B) Leave out the NAF-ID

The UE could be made responsible to assign a short (i.e. one byte) MUK-ID **uniquely from UE point of view over all BM-SC**. This assumes that the BM-SC can store the data in an IMSI related way. One byte would suffice for encoding 256 IDs, 2 bytes would suffice for distinguishing between 65536 different keys at the UE. An advantage is that it guarantees the unique MUK-ID assignment using a limited number of bytes, which is much shorter than solutions including RAND and/or NAF-ID.

This solution also (cf A.2) requires that the assigned MUK-ID shall be transported within the first http request that is initiated by the UE using that new generated NAF key.

Can this solution also be used for MRK-ID ?

TS 33.246 section 6.2.1 currently reads:

> *When the user wants to join (or leave) an MBMS user service, it shall use HTTP digest authentication RFC 2617 [8] for 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 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 client payload of HTTP Digest message.*

The use of the B-TID as username actually means that the MRK (i.e. the user) is identified by the B-TID pseudonym. With the B-TID solution for username, the BM-SC always needs to store the B-TID (RAND + BSF name) together with the GBA-derived keys. In stead of using a long B-TID, the BM-SC could generate a MRK-ID from his viewpoint and transport it within the http 200 OK that completes the bootstrapping. This would allow the BM-SC to store a short MRK-ID (much shorter than B-TID). The key lifetime of the associated keys will still apply. A failed authentication using this short username should always be followed by a re-attempt using a B-TID.

Subsequent http requests after a successful B-TID use, can then use the shorter MRK-ID i.e. the user name assigned by BM-SC. A different realm can distinguish between the use of the B-TID and the MBMS assigned username. MIKEY Key deliveries can use the UE-assigned MUK-ID.

The UE should still know towards which BM-SC the MRK can be used, this means that the MRK should be tagged to the NAF-ID within the UE. This is done anyhow at NAF key derivation when completing the bootstrapping.

An advantage is that it allows the BM-SC to forget the bootstrapping information (e.g. B-TID) after having generated the MUK keys, hence it contributes in lowering the required storage capacity at the BM-SC. How the UE and the BM-SC assign the MUK-ID and MRK-ID needs not be standardized.

4 Conclusions

The analysis concluded that the MUK cannot be identified from UE point of view by only using the NAF-ID within a MIKEY message. Three solutions were analysed for MUK identification over Ua

a) Base64encoded(RAND)@NAF-ID

b) UE_assigned@NAF-ID

c) Using one or two byte identification uniquely assigned by the UE over all BM-SC.

Proposal c and b come at the expense of an extra http field, and requires UE functionality to generate and store the shorter MUK-ID. Option c is preferred over option b.

Also the use of a shorter username than the B-TID (Base64encoded(RAND)@BSF) within the http request to the BM-SC is possible. This again comes at the expense of extra http field (now in the http response) but allows the BM-SC to forget the B-TID after its first successful use. Again the UE/BM-SC have to store the new identifier during the lifetime of the GBA-Key.

Introducing a short MUK-ID (option c) without a shorter username than B-TID for MRK, does not lead to any storage savings at the BM-SC. Saving some MIKEY bytes is not seen as a sufficient advantage for the implementation of additional functionality.

Two change requests are presented in attach to this contribution. Attachment 1 implements option a, attachment 2 implements option c together with the shorter username possibility. SA3 is asked to consider the above argumentation and approve one of the attached CRs.

3GPP TSG-SA3 Meeting #36
Shenzhen, China, 23-26 October 2004

Tdoc ⌘Att1_S3-041012

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **031** ⌘**rev** **-** ⌘ Current version: **6.0.0** ⌘

*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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Specify how to identify the MUK
Source:	⌘	Siemens
Work item code:	⌘	MBMS
Date:	⌘	16/11/2004
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 currently not specified how the MUK is identified within MIKEY messages
Summary of change:	⌘	Add the missing text
Consequences if not approved:	⌘	

Clauses affected:	⌘	New clause 6.2.0			
Other specs affected:	⌘	**Y**	**N**		
			N	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

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.

6.2.0 MUK Identification

The key MUK shall be identified in NAI format as base64encoded(RAND)@NAF-ID.

6.2.1 Authentication and authorisation in application level joining

When the user wants to join (or leave) an MBMS user service, it shall use HTTP digest authentication RFC 2617 [8] for 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 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 client payload of HTTP Digest message.

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.

6.2.2 Authentication and authorisation in MBMS bearer establishment

The authentication of the UE during MBMS bearer establishment relies on the authenticated point-to-point connection with the network, which was set up using network security described in TS 33.102 [4] or TS 43.020 [12]. Authorisation for the MBMS bearer establishment happens by the network making an authorisation request to the BM-SC to ensure that the UE is allowed to establish the MBMS bearer(s) corresponding to an MBMS User Service (see TS 23.246 [3] for the details). As MBMS bearer establishment authorisation lies outside the control of the MBMS bearer network (i.e. it is controlled by the BM-SC), there is an additional procedure to remove the MBMS bearer(s) related to a UE that is no longer authorised to access an MBMS User Service.

6.2.3 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 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.

3GPP TSG-SA3 Meeting #36
Shenzhen, China, 23-26 October 2004

Tdoc ⌘Att2_S3-041012

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **032** ⌘**rev** **-** ⌘ Current version: **6.0.0** ⌘

*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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Specify how to identify the MUK and MRK
Source:	⌘	Siemens
Work item code:	⌘	MBMS
Date:	⌘	16/11/2004
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 currently not specified how the MUK is identified within MIKEY messages The username within http requests to the BM-SC can be shortened which saves database capacity within the BM-SC
Summary of change:	⌘	Add the missing text on MUK-ID Specify how a shorter username can be used (MRK-ID)
Consequences if not approved:	⌘	

Clauses affected:	⌘	6.2.1, New clause 6.2.0			
		Y	**N**		
Other specs Affected:	⌘		**N**	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

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.

6.2.0 MUK and MRK Identification

The MUK-ID is generated by the UE and shall be unique towards all BM-SC that the UE is communicating with.

The MUK-ID is one BYTE long.

The MRK-ID shall be generated by the BM-SC. The MRK-ID will be used as short username in http request towards the BM-SC.

6.2.1 Authentication and authorisation in application level joining

When the user wants to join (or leave) an MBMS user service, it shall use HTTP digest authentication RFC 2617 [8] for 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 following adaptations apply to HTTP digest with B-TID as username:

- 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 and MUK-ID are~~is~~ specified in client payload of HTTP Digest message
- ~~.~~ a short username (MRK-ID) is transported within the 200 OK response and shall be used as username in subsequent http requests.

The following adaptations apply to HTTP digest with MRK-ID as username:

- the MRK-ID is used as username;
- MRK (MBMS Request Key) is used as password;
- the joined MBMS user service is specified in client payload of HTTP Digest message

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.

6.2.2 Authentication and authorisation in MBMS bearer establishment

The authentication of the UE during MBMS bearer establishment relies on the authenticated point-to-point connection with the network, which was set up using network security described in TS 33.102 [4] or TS 43.020 [12]. Authorisation for the MBMS bearer establishment happens by the network making an authorisation request to the BM-SC to ensure that the UE is allowed to establish the MBMS bearer(s) corresponding to an MBMS User Service (see TS 23.246 [3] for the details). As MBMS bearer establishment authorisation lies outside the control of the MBMS bearer network (i.e. it is controlled by the BM-SC), there is an additional procedure to remove the MBMS bearer(s) related to a UE that is no longer authorised to access an MBMS User Service.

6.2.3 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 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.