3GPP TSG SA WG3 Ad hoc **S3z030027**

3 - 4 September 2003

Antwerp, Belgium

Agenda Item:	MBMS
Source:	Ericsson
Title:	Introducing MIKEY in TS 33.246
Document for:	Discussion/Decision

1. Scope

This contribution and accompanying pseudo CR [1] discuss and describe how MIKEY can be used as key management protocol for MBMS. It is proposed to include the suggested text in the companion pseudo CR to the MBMS Security TS 33.246 [2] to show that a complete solution is available. This contribution also addresses the concerns that were raised in SA3#29 towards MIKEY.

2. Introduction

Background from SA3#29

In SA3#29 Ericsson presented contribution [3] and related pseudo CR, which proposed to adopt SRTP and MIKEY for MBMS. Proposal was not agreed due to concerns raised in the meeting.

This contribution and accompanying pseudo CR address the concerns raised in SA3#29 and describe how MIKEY can be used as key management protocol for MBMS. It is proposed to include the suggested text in the companion pseudo CR to the MBMS Security TS 33.246 [2] to show that a key management solution is available.

SRTP is discussed in another Ericsson contribution in the present meeting [4].

Earlier background

In SA3#25 Ericsson presented contributions [5] and [6] which proposed to adopt SRTP and MIKEY for MBMS.

[6] discussed MIKEY and it was compared to two other multicast key management protocols, namely Group Domain of Interpretation (GDOI) [7] and Group Security Association And Key Management Protocol (GSAKMP-light) [7]. MIKEY was found the most efficient and best suitable for MBMS since it is using pre-shared keys with symmetric cryptography. MIKEY was proposed for MBMS.

In [5] SRTP was compared against IP sec and radio –level multicast security. The contribution proposed SRTP as security protocol for streaming applications for MBMS.

However, SA3 #25 concluded that there were too many open issues regarding e.g. the security architecture and further contributions were requested to progress the technical specification. At that time the TS was not mature enough for specific protocols to be included.

In meetings #27 and #28 SA3 agreed on some important security architecture issues, namely that the encryption of MBMS traffic shall be done between UE and BM-SC and that the BM-SC shall be the entity to generate and distribute the traffic encryption key (TEK) to the UEs [8]. Today many issues are still to be specified, e.g. regarding authentication architecture, charging models (and related keying mechanisms) and Gmb interface functionality.

Ericsson presented a discussion paper [9] on the status of MIKEY [10] and SRTP [11] in IETF in SA3#28. These protocols are strong candidates for key management and security protocols for MBMS and they are likely to get RFC status during 2003.

2. Discussion

Authenticating and authorizing the user

In [3] Ericsson presented the relation between MSEC architecture and the MBMS architecture and proposed MBMS work to adopt the MSEC architecture principles.

Ericsson presented a paper in SA3#29 on authentication [12]. Currently discussion is ongoing on the generic authentication architecture (GAA). Figure 1 shows a generic authentication architecture that is discussed in [13] in the present meeting.

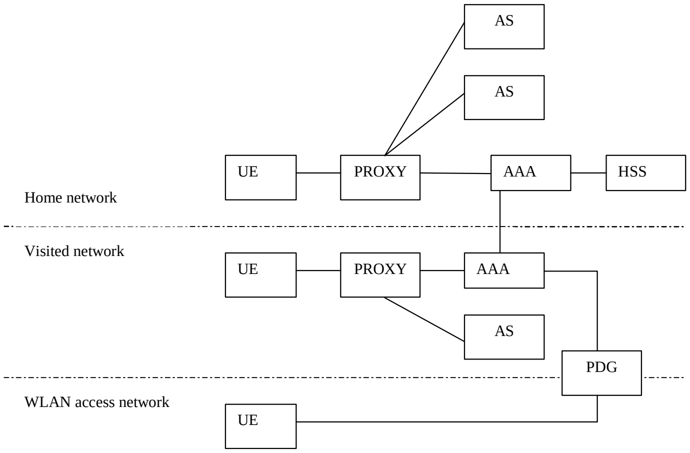

Figure 1: GAA based on AAA

Key management and distribution

Decryption keys should be distributed only to authorised users. Therefore key management has a close relation to user authentication and authorisation. Figures 2 and 3 show an example how MIKEY can be used for key management in the generic authentication architecture. MIKEY is not dependent on any specific authentication architecture. It can conform to many different authentication mechanisms. I.e. choosing MIKEY does not restrict the authentication architecture.

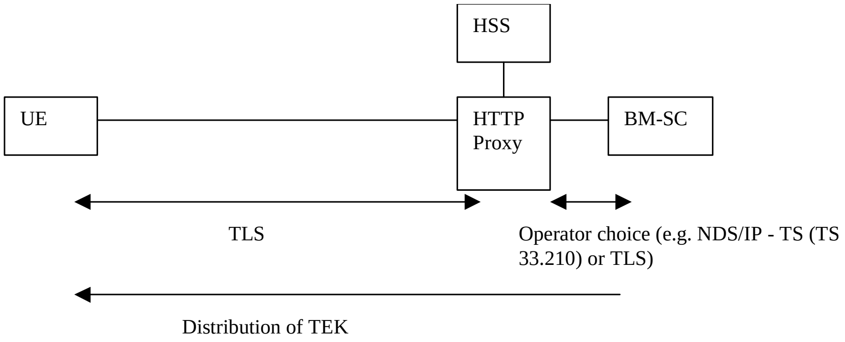

Figure 2: TEK distribution in GAA

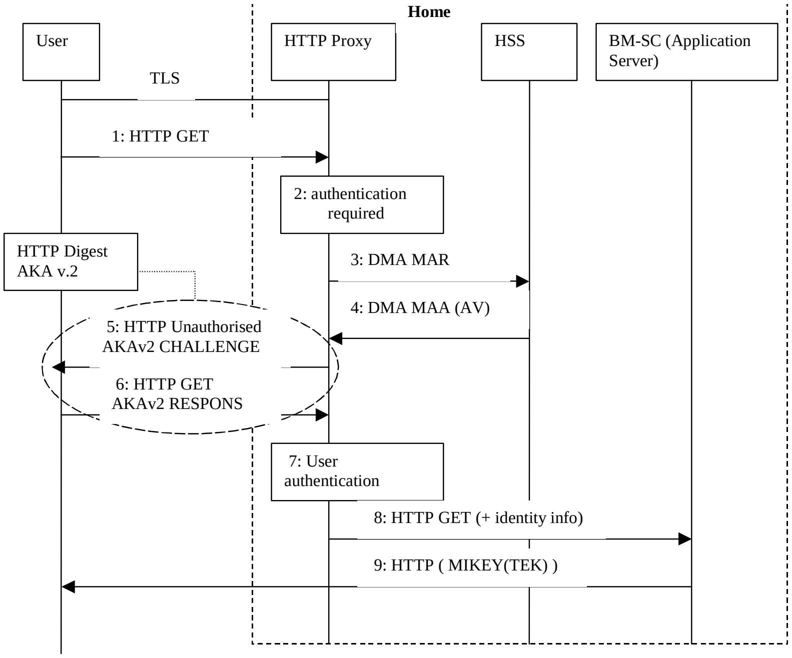
Home
User
HTTP Proxy
HSS
BM-SC (Application Server)
TLS
1: HTTP GET
2: authentication required
HTTP Digest AKA v.2
3: DMA MAR
4: DMA MAA (AV)
5: HTTP Unauthorised AKAv2 CHALLENGE
6: HTTP GET AKAv2 RESPONS
7: User authentication
8: HTTP GET (+ identity info)
9: HTTP (MIKEY(TEK))

Figure 3: Messages in TEK distribution in GAA

Note: DMA MAR & MAA: Commands of Diameter Multimedia Application currently developed in IETF, see more in (draft-belinchon-aaa-diameter-mm-app-01.txt)

Point-to-point versus point-to-multipoint

Lately many contributions have been seen on keying issues in the latest SA3 meetings. The discussion has been concerning mainly whether re-keying should be done as point-to-point transmission or as point-to-multipoint transmission between the BM-SC and the UE(s).

It has been stated that point-to-multipoint re-keying uses resources more efficiently since it uses multicast and it probably is a feasible choice in the long run. For future interoperability and taking into account also other access technologies the chosen multicast keying mechanism should be based on IETF multicast key management protocols. However, the development of point-to-multipoint mechanisms, such as Logical Key Hierarchy (LKH) [14], is in early stages in IETF and is not awaited to be finalized in the timeframe of 3GPP Release 6, which is the first release for MBMS services. Introducing point-to-multipoint re-keying mechanism would also add extra complexity to the system and possibly endanger the timetable for Release 6. Introducing only point-to-point mechanism in Release 6 does not mean that point-to-multipoint mechanism is excluded from the system. Indeed point-to-multipoint could be regarded as a more optimized “next phase” re-keying mechanism, which could be introduced in later phases if required. Therefore it is important that Release 6 system should be designed so that point-to-multipoint mechanism could be introduced in later releases, if required, and that these two mechanisms could probably co-exist.

Based on the reasoning above point-to-point re-keying mechanisms should be considered for Release 6 MBMS service. Point-to-point mechanism is said to suffer from scalability problems when users have to be re-keyed individually. Therefore, such mechanisms need to be developed that this problem is overcome. Some ideas for this could be e.g.

- Sending many keys at one re-key message
- Spreading individual re-keying requests randomly within an interval
- Scheduling the users to request new keys so that no overlap occurs
- Distributing BM-SC functionality to several entities

MIKEY can carry several keys. It cannot currently support LKH mechanisms but it can be extended to support LKH, which requires extensions (either specified in 3GPP or by an IETF RFC). This contribution discusses point-to-point re-keying. Point-to-multipoint is FFS.

Reliable key delivery

The reliable delivery of keys to the UEs is important for secure multicast systems for example for charging reasons. There are in practice two ways to do it: Either the re-keying mechanism has functionality for reliable key delivery or the re-keying mechanism relies on the underlying transport to be reliable.

Doing re-keying reliably over point-to-multipoint may cause scalability problems since all UEs need to acknowledge the delivery. Reliable multicasting in general is a hard problem.

If re-keying is done point-to-point, there are better chances to assure reliable transport. E.g. when MIKEY is run over HTTP, TCP is used and thus the reliable delivery is in place.

Qualcomm introduced a key management scheme called BAK in [15]. When protecting the MBMS data, the BAK scheme uses short-term keys SK, which are derived from a long-term key BAK and a random number SK_RAND sent along with the MBMS data.

When it comes to reliable key delivery, the BAK scheme does not specify how to implement reliable delivery for BAK key or SK_RAND value. When the SK_RAND is changed too often, there is probably no time for redundancy, such as retransmitting a lost SK_RAND value. This will likely lead to incomplete data reception, i.e. that the UE will not be able to decrypt parts of the received MBMS data.

Features of MIKEY

MIKEY [10] is a key management protocol, which is designed to provide key management for secure multimedia sessions. It can be used for streaming as well as for downloading /messaging scenarios.

The design goals of MIKEY have been: end-to-end security; simplicity; efficiency (low bandwidth consumption, low computational workload, small code size and minimal number of roundtrips); tunnelling (possibility to tunnel/integrate MIKEY to session establishment protocols, e.g. SIP [16] and RTSP [17]); independent of any specific security functionality of the underlying transport.

Regarding the applicability to different security protocols MIKEY supports currently only SRTP but it can be extended to support other protocols also, e.g. IPSec. Extension requires another RFC though. Ericsson proposes to use SRTP for streaming MBMS applications in [4]. The security protocol for MBMS download is FFS.

MIKEY has no identity protection and will therefore need to rely on external mechanisms for identity protection.

When the TEK is carried in the MIKEY message, it can be protected with KEK (Key Encryption Key). It is FFS if TLS could be used as a protection mechanism for TEK distribution.

It should be noted that MIKEY is not dependent on any specific authentication architecture. It can conform to many different authentication mechanisms. I.e. choosing MIKEY does not restrict the authentication architecture.

Concerns on MIKEY

In the following some concerns are clarified that were raised in SA3#29:

1. **MIKEY cannot be put into the main body of the draft TS as SA3 has not decided about higher level issues**

Both the MBMS work and MBMS specification need to be proceeded to reach the milestones for Release 6. MIKEY is a concrete proposal for key management. Other seen proposals e.g. [18], [15] have not specified e.g. the needed protocols or detailed mechanisms. Regarding point-to-multipoint re-keying MIKEY can be extended to support Logical Key Hierarchy (LKH) also the future. See also chapter 2.3.1 for discussion on point-to-multipoint.

2. **Every time you have to re-key you have to do much signalling**

The signalling load problem is not specific for MIKEY but it is common for all point-to-point mechanisms. Solutions have been proposed to overcome this problem in the present contribution, e.g. sending many keys at one re-key message, spreading individual re-keying requests randomly within an interval, scheduling the users to request new keys so that no overlap occurs. However, these are FFS. See also chapter 2.3.1 for discussion on point-to-multipoint.

3. **Is harmonization with 3GPP2 important for this issue (3GPP2 uses the BAK scheme)?**

Ericsson has regarded harmonization with IETF as an important issue. Ericsson would also like to see on protocol level how the harmonization with 3GPP2 could be done.

4. **Are there MIKEY implementations available?**

Ericsson has a basic implementation of MIKEY that will be published soon.

5. **Is there a possibility for congestion in the HSS due to re-keying?**

As indicated in concern 2, this is not only MIKEY specific problem. The access rate to HSS depends also on the chosen authentication architecture. There are possible solutions to overcome this problem, see also concern 2.

Status of MIKEY in IETF

MIKEY has passed IESG Security review and the IESG last call. MIKEY is now in the queue waiting for the final IESG review. An RFC is likely to be published during 2003.

3. Proposal

It is proposed that SA3 makes a working assumption to choose MIKEY as a key management protocol for MBMS and that the description on MIKEY in the pseudo CR is included in TS 33.246 in chapter 6.

4. Conclusion

This contribution has given reasoning for choosing MIKEY as key management protocol for MBMS and introducing it to TS 33.246. Companion CR [1] describes the proposed changes to TS 33.246.

5. References

[1] TD S3-030xxx, Pseudo CR Introducing MIKEY to TS 33.246, Ericsson

[2] 3GPP TS 33.246, v 0.2.0 Security of Multimedia Broadcast Multicast Service

[3] TD S3-030368, Introducing MIKEY and SRTP in TS 33.246, Ericsson

[4] TD S3-030xxx, Introducing SRTP in TS 33.246, Ericsson

[5] TD S3-020533, Security protocol, Ericsson

[6] TD S3-020534, Key management, Ericsson

[7] http://www.ietf.org/html.charters/msec-charter.html

[8] TD S3-030249, Key generation and distribution in MBMS, Ericsson

[9] TD S3-030250, Status of SRTP and MIKEY in IETF, Ericsson

[10] MIKEY: Multimedia Internet KEYing, draft-ietf-msec-mikey-07.txt, work in progress

[11] The Secure Real-time Transport Protocol, draft-ietf-avt-srtp-09.txt, work in progress

[12] TD S3-030367, Access to Application Servers using HTTP in MBMS, Ericsson

[13] TD S3-030xxx, Generic Authentication Architecture based on AAA and AKAv2, Ericsson

[14] IETF RFC 2627, Key management for Multicast: Issues and Architecture, June 1999

[15] TD S3-030356, MBMS Security Framework, Qualcomm

[16] IETF RFC 3261, SIP: Session Initiation Protocol

[17] IETF RFC 2326, Real time Streaming Protocol (RTSP)

[18] TD S3-030396, Key distribution and billing in PayTV model, GemPlus

3GPP TSG-SA3 Ad hoc **Tdoc ⌘S3-030xxx**
Antwerp, Belgium, 3 - 4 September, 2003

CR-Form-v7

CHANGE REQUEST

⌘	**33.246**	**CR**		⌘ **rev**	**-**	⌘	Current version:	**0.0.3** ⌘

*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:	⌘	Introducing MIKEY to TS 33.246		
Source:	⌘	Ericsson		
Work item code:	⌘	MBMS	***Date:*** ⌘	2003-08-29
Category:	⌘	**D**	***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:* *2 (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)*

Reason for change:	⌘	In order to enhance the TS, it is proposed to add descriptions how key management is implemented with MIKEY.
Summary of change:	⌘	The following descriptions are added: - Key management with MIKEY It is also decribed how key activation is indicated in SRTP data stream.
Consequences if not approved:	⌘	

Clauses affected:	⌘	6				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

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 TR 23.846: " Multimedia Broadcast/Multicast Service; Architecture and Functional Description".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 23.246: " Multimedia Broadcast/Multicast Service; Architecture and Functional Description".

[6] MIKEY: Multimedia Internet KEYing, Internet Draft

********* NEXT PROPOSED CHANGE *********

3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.

Subclause numbering depends on applicability and should be renumbered accordingly.

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply.

example: text used to clarify abstract rules by applying them literally (place saver to retain format).

TEK – Traffic Encryption Key: the common encryption key, encrypting the MBMS traffic broadcasted to all users.

KEK – Key Encryption Key: the pre-shared encryption key in the UE and the network node (i.e. BM-SC) is, a) used by the network node to encrypt the TEK before distributing the TEK to the UE; and b) used by the UE to decrypt the TEK received from the BM-SC. Whehther the KEK is the same as CK or derived from CK is FFS.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol>	<Explanation>

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

KEK	Key Encryption Key
MBMS	Multimedia Broadcast/Multicast Service
TEK	Traffic Encryption Key

********* NEXT PROPOSED CHANGE *********

6.2 Key management

Editor's note: this section will contain the details of how the keys are updated in a Multicast Service

Editor's note: The key management mechanisms and detailed procedures are currently under investigation and they may change depending on e.g. chosen charging models.

Editor's note: The MIKEY key management mechanisms presented here use SRTP, since MIKEY is originally designed to support SRTP. SRTP is one candidate for security protocol for streaming MBMS data. MIKEY can be extended to support other security protocols aswell. Usage of MIKEY with download scenarios is expected to be very similar with streaming scenarios. However this is FFS since security protocol for download applications is FFS.

6.2.1 General

The multicast data of a specific MBMS service is protected with a common traffic encryption key (TEK). The TEK is distributed to all the UEs that have registered to the MBMS service in order for the UEs to be able to decrypt the encrypted multicast data sent from the BM-SC.

The TEK is generated by the BM-SC and distributed to the UEs using the MIKEY [6] protocol. MIKEY is carried over HTTP over TCP.

Editor's note: How to carry MIKEY over HTTP needs to be specified in as a HTTP profile in 3GPP.

When the TEK is distributed to the UEs, it is protected by the BM-SC with a Key Encryption Key (KEK) and encapsulated into MIKEY message. The KEK is unique shared secret between a UE and the BM-SC, i.e. it is not common to all UEs in the group. The UE and the BM-SC retrieve the KEK during the authentication procedure. E.g. it can be the CK resulting from the Digest AKA procedure between the UE and the BM-SC or the KEK can be derived from the CK.

Editor's note: How to derive the KEK from, e.g. CK is FFS.

Editor's note It is FFS if TLS could be used as a protection mechanism for TEK distribution.

The key management can be separated in two parts, initial keying and the re-keying.

6.2.2 Initial keying

The initial keying happens point to point between the UE and the BM-SC when the UE registers to the MBMS service. In the initial keying the UE receives the TEK from the BM-SC in order to be able to decrypt the encrypted MBMS data sent from the BM-SC. The UE has to be authenticated and authorised for the specific MBMS service before the TEK is distributed to it.

Note that the IGMP Join message is considered as a join request for the nearest router (i.e. GGSN) [*not* for the application server (i.e. BM-SC)] in order for the to GGSN to enable multicast transmission towards the UE. The GGSN may need to perform authorisation towards the BM-SC, but this authorisation is made in order to trigger the MBMS context activation and resource reservation procedures towards SGSN and RAN. The MBMS application in UE is authorised to the MBMS service during the authentication when it gets the TEK.

Editor's note: If a UE is registering for a second (or n:th) MBMS service to the same BM-SC, it should not be authenticated again, but only authorised for the requested service. This saves authentication vectors and signalling burden especially on the radio interface.

The initial keying procedure is as follows

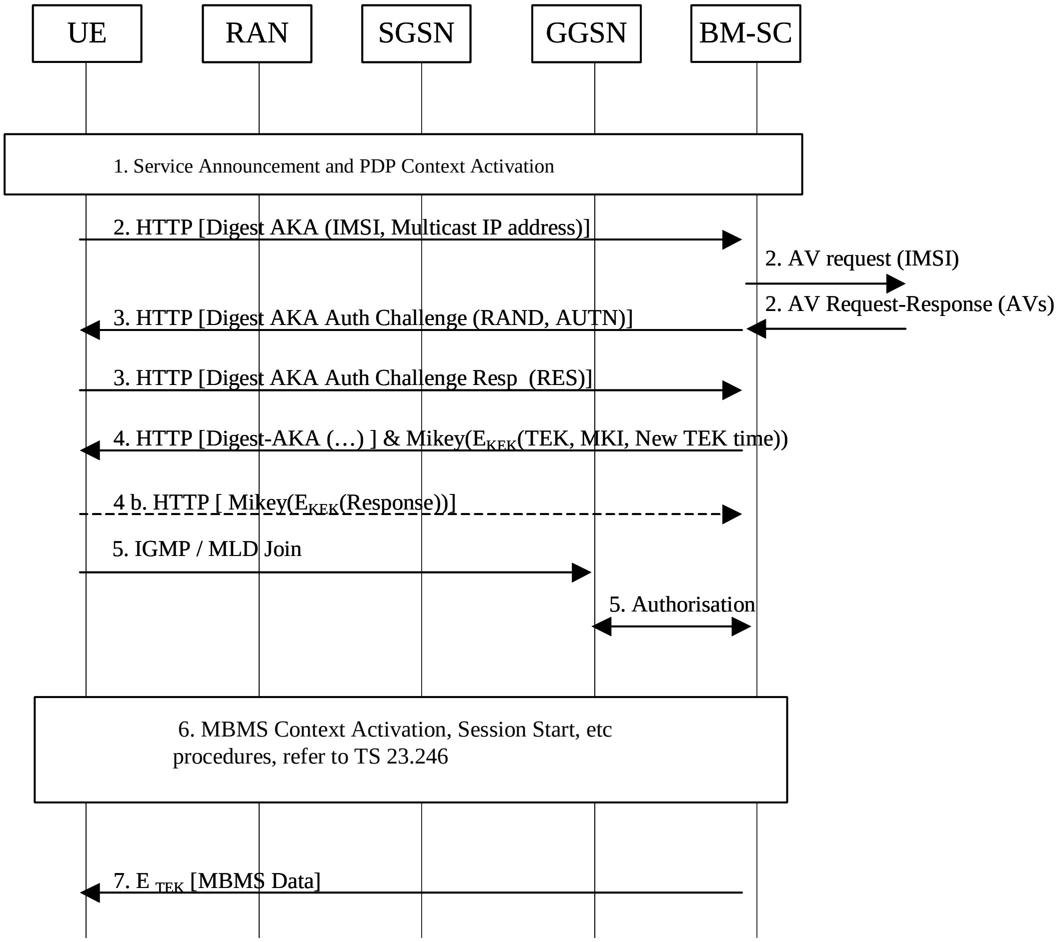
UE
RAN
SGSN
GGSN
BM-SC
1. Service Announcement and PDP Context Activation
2. HTTP [Digest AKA (IMSI, Multicast IP address)]
2. AV request (IMSI)
2. AV Request-Response (AVs)
3. HTTP [Digest AKA Auth Challenge (RAND, AUTN)]
3. HTTP [Digest AKA Auth Challenge Resp (RES)]
4. HTTP [Digest-AKA (…)] & Mikey(E_{KEK}(TEK, MKI, New TEK time))
4 b. HTTP [Mikey(E_{KEK}(Response))]
5. IGMP / MLD Join
5. Authorisation
6. MBMS Context Activation, Session Start, etc procedures, refer to TS 23.246
7. E_{TEK} [MBMS Data]

Figure 1 Initial keying

Note: The user is authenticated depending on the chosen authentication framework. MIKEY is not dependent on any specific authenticatin architecture. It can conform to many different authentication mechanisms. *This procedure uses HTTP Digest AKA only as an example.*

1. It is assumed that the UE has learnt the multicast IP address of the service and the IP address of the BM-SC from the service announcement. It is also assumed that the regular PDP context has been setup.

2. The user sends a HTTP request (HTTP GET [IMSI, Multicast IP address]) to register to a specific MBMS service to the BM-SC via the general purpose PDP context.

3. The BM-SC initiates a HTTP Digest AKA authentication challenge towards the UE. The UE responds. Note that the detailed authentication procedure is described in chapter x.x.

4. When the UE has responded successfully to the challenge, the BM-SC makes a check whether the UE is authorised to receive this MBMS service. If the UE is authorised for the specific MBMS service, the BM-SC sends the following parameters encrypted with KEK in a MIKEY message to the UE. Refer to point 4 in figure 1:

- Traffic encryption key (TEK);

- Master Key Identifier (MKI), which identifies the TEK. This is used in the security protocol (e.g. SRTP for streaming) to indicate which TEK is in use. From the MKI the UE sees when a new TEK has been taken into use. The UEs must have received the new TEK before the TEK is activated in the multicast data transmission;

Editor's note: The exact mechanisms how the UEs fetch the new TEK without causing congestion (e.g. overloading the BM-SC) is under investigation.

Editor's note: The MIKEY key management mechanisms presented here use SRTP, since MIKEY is originally designed to support SRTP. SRTP is one candidate for security protocol for streaming MBMS data. MIKEY can be extended to support other security protocols aswell.
Usage of MIKEY with download scenarios is expected to be very similar with streaming scenarios. However this is FFS since security protocol for download applications is FFS.

- Time to fetch a new TEK. This is a time specified by the BM-SC when the UE has to fetch new TEK in order to avoid congestion when UEs fetch new keys;

Editor's note: The current view is to use time specified by BM-SC. Another possibility enabled by MIKEY is to use an SRTP Sequence Number value to indicate the time to fetch a new TEK. These alternatives need further investigation.

Editor's note: A parameter for "Lifetime of the TEK" may not be needed since the exact activation of the new TEK is indicated when the MKI changes in received encrypted data packets (e.g. in SRTP packets) and the UE knows when to fetch the new key from the "Time to fetch a new TEK" parameter.

Editor's note: MIKEY has an optional Response message, which could be used to ensure the delivery of TEK to the UE. It is shown as 4b) in the figure above. Whether this message could be applicable for MBMS is FFS.

5. The UE sends IGMP / MLD Join message over the regular PDP context in order to signal its interest in receiving a specific MBMS service identified by a multicast IP address.
Note that the IGMP Join message is considered as a join request for the nearest router (i.e. GGSN) [*not* for the application server (i.e. BM-SC)] in order for the to GGSN to enable multicast transmission towards the UE. The GGSN may need to perform authorisation towards the BM-SC, but this authorisation is made in order to trigger the MBMS context activation and resource reservation procedures towards SGSN and RAN. The MBMS application in UE is authorised to the MBMS service during the authentication when it gets the TEK.

6. The MBMS Context Activation, Session Start, etc procedures until the data transmission phase are out of the scope of this TS. Refer to TS 23.246 [5].

7. The BM-SC sends streaming MBMS multicast data. It is carried over SRTP [7]. The MKI field is present and it specifies the used TEK. The UE decrypts the received data.

6.2.3 Re-keying

6.2.3.1 General

Different reasons for re-keying include e.g. group membership changes, creation of new keys, expiration of keys or then a user that has been “offline” during the latest re-keying may want to re-synchronize the keys. Applicable re-keying mechanism depends among other things on the chosen charging models, which are currently FFS.

Re-keying procedure includes two phases: a) actual re-keying, i.e. sending the new TEK to the UEs and b) activating the new TEK.

6.2.3.2 Re-keying

Re-keying is performed point to point between each UE and the BM-SC.

When time to fetch a new TEK comes, UE requests a new TEK from the BM-SC. MIKEY does not include a specific re-key request message but the UE needs to make a “re-registration” request by sending a HTTP request to the BM-SC. The network may perform authentication procedures depending on the authentication framework. Refer to point 2 in figure 1.

The congestion problem when requesting new TEKs is FFS. It can be overcome by e.g.

- Sending many keys at one re-key message
- Spreading individual re-keying requests randomly within an interval
- Scheduling the users to request new keys so that no overlap occurs
- Distributing BM-SC functionality to several entities

The BM-SC sends similar parameters as in the registration phase to the UE encrypted with KEK in a MIKEY message:

- Traffic encryption key (TEK);
- Master Key Identifier (MKI), which identifies the TEK. This is used in the security protocol (e.g. SRTP for streaming) to indicate which TEK is in use. From the MKI the UE sees when a new TEK has been taken into use. The UEs must have received the new TEK before the TEK is activated in the multicast data transmission;

Editor’s note: The exact mechanisms how the UEs fetch the new TEK without causing congestion (e.g. overloading the BM-SC) is under investigation.

- Time to fetch a new TEK. This is a time specified by the BM-SC when the UE has to fetch new TEK in order to avoid congestion when UEs fetch new keys;

Editor’s note: The current view is to use time specified by BM-SC. Another possibility enabled by MIKEY is to use an SRTP Sequence Number value to indicate the time to fetch a new TEK. These alternatives need further investigation.

Editor’s note: A parameter for “Lifetime of the TEK” may not be needed since the exact activation of the new TEK is indicated when the MKI changes in SRTP packets and the UE knows when to fetch the new key from the “Time to fetch a new TEK” parameter.

6.2.3.3 Activation of new TEK

It is assumed that the UEs have fetched the new TEK before the new TEK is activated.

Editor's note: The exact mechanisms how the UEs fetch the new TEK without causing congestion (e.g. overloading the BM-SC) is under investigation.

The received encrypted data packets (e.g. SRTP packets) include the MKI field, which identifies the current TEK.

When a new TEK is activated, the BM-SC updates the MKI respectively in the sent data packets.

The exact activation of the new TEK is indicated when the MKI changes in SRTP packets.

UEs notice the MKI change in the received encrypted data packets (e.g. in SRTP stream) and can thus activate a correct TEK for decrypting the received data.

UEs that have been out of radio coverage and may therefore have dropped out of key synchronisation from the current TEK can notice that the MKI in the received encrypted data packets is unknown for them. These UEs can then request a new TEK from the BM-SC. It is FFS whether this is needed for streaming services.