3GPP TSG SA WG3 Security — SA3#36 **S3-040995**

November 23 - 26, 2004

Shenzhen, China

Title: **IETF work needed for MBMS security**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **MBMS**

1 Introduction

In SA3 #35 meeting in Malta Ericsson volunteered to initiate the IETF processes for reserving official name space for MBMS extensions in RFC 3830 [1] (MIKEY) and for reserving UDP port number for MIKEY. Ericsson has submitted an internet draft (attached to this contribution [2]) to IETF and has started the UDP port registration process. This contribution explains the content and status of these processes.

2 MBMS extensions for MIKEY in IETF

Chapters 2.1 and 2.2 show the current situation and related problems with the MBMS extensions needed to MIKEY RFC. Chapter 2.3 describes how these problems are solved in the internet draft submitted by Ericsson to IETF.

2.1 Current situation

Current TS 33.246 [3] and approved CR S3-040857 [4] from Malta meeting identify three places in RFC 3830 where new name space is needed for MIKEY's MBMS extensions. These extensions are needed to distinguish MSK delivery from MTK delivery and to identify "outer" and "inner" keys:

1. Data type field in common header (section 6.1 of MIKEY). New name space is needed to indicate if the message carries MSK or MTK.

2. General extension payload (section 6.15 of MIKEY). New general extension payload type is needed to carry the identifiers of the "outer key" that is used to protect the message and "inner key" that is carried in the message. In case of MSK delivery the "outer key ID" and the "inner key ID" are MUK-ID and MSK-ID, respectively. In case of MTK delivery, these are MSK ID and MTK ID, respectively.

3. Type field in Key data sub-payload (section 6.13 of MIKEY). New name space is needed to indicate if the message carries MSK or MTK.

2.2 Problem statement

A problem with bullets 1 and 3 is that they do not follow the semantics of original MIKEY fields. This is analysed below.

2.2.1 Data Type field

MIKEY protocol supports three key delivery methods: pre-shared key, public key and Diffie-Hellman methods. The Data Type field indicates which method is used. The current values of Data Type field in RFC 3830 are as follows:

Table 1. MIKEY Data Type Values in RFC 3830

Data Type	Value	Comment
Pre-shared	0	Initiator's pre-shared key message
PSK ver msg	1	Verification message of a Pre-shared key message
Public key	2	Initiator's public-key transport message
PK ver msg	3	Verification message of a public-key message
D-H init	4	Initiator's DH exchange message
D-H resp	5	Responder's DH exchange message
Error	6	Error message

MBMS security is using the pre-shared key method as is specified in clause 6.4.2 of TS 33.246: "*MIKEY shall be used with pre-shared keys as described in RFC 3830 [9]*."

Therefore it would be natural that corresponding Data Type field values (0 and 1) are used also for MBMS security instead of that new Data Type values would be defined for MSK or MTK delivery. This kind of modification that is against the semantics of a field would also be very hard to get accepted in IETF. Instead, the MSK/MTK indication could be carried in the extension payload, see chapter 2.3.

2.2.2 Type field in key data sub-payload of KEMAC

CR S3-040857 introduced that the Type field in Key data sub-payload in KEMAC payload also carries the indication whether the message carries MSK or MTK. However, this is not needed for the following reasons:

- The key type is indicated already by other fields in the message, i.e. in Data Type field in current TS or in extension payload as proposed in this contribution. Also MGV-F (e.g. UICC) receives this information since the whole MIKEY message is conveyed to the MGV-F.

- The Type field is used to indicate whether MIKEY needs to further derive the transported key. For example in case of streaming further key derivation from MTK is not needed, since SRTP has its internal key derivation. But in case of download, MIKEY may need to derive MTK_I and MTK_C from MTK. This can be indicated by using value "TEK" for streaming case and "TGK" for download case, see table 2 below.

Table 2. MIKEY Type Values in Key data sub-payload

Type	Value
TGK	0
TGK + SALT	1
TEK	2
TEK + SALT	3

2.3 Proposed extension payload

2.3.1 Internet draft

An internet draft [2] was submitted by Ericsson to the IETF meeting number 61. It may be too early to estimate when the draft gets into RFC status. The internet draft is described in the following. It proposes to concentrate all needed MBMS extensions to the general extension payload, i.e. key type and key identifier are carried close to each other in new general extension payload type.

A new type of general extension payload is defined is as follows:

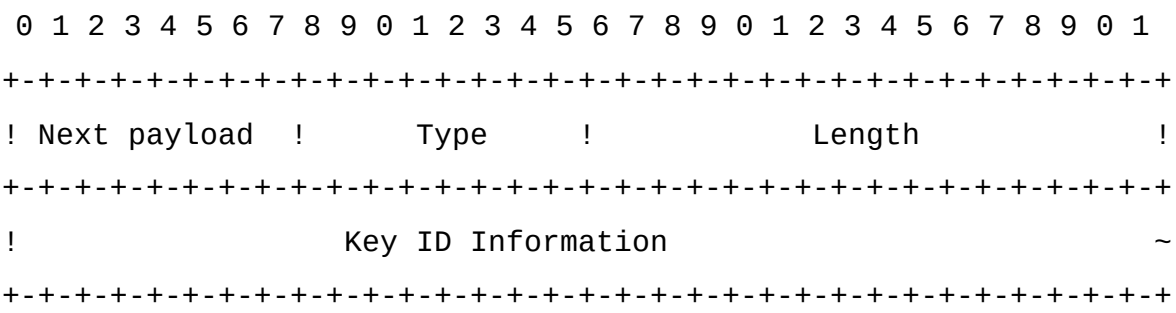


Figure 1. New general extension payload

Values ‘0’ and ‘1’ are already used therefore a new value ‘2’ is proposed for the Type. (The value may change when the draft evolves since also another new general extension payload type has been proposed in IETF.)

The Key ID Information field consists of one or more Key Type ID sub-payloads as described below.

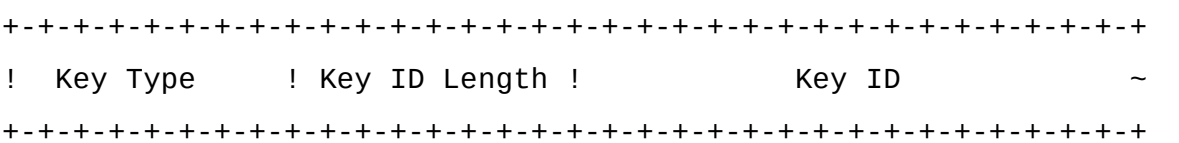


Figure 2. Key Type ID subpayload

The following values are specified for the Key Type field:

Table 3. Key Type Values in Key Type ID sub-payload

Key Type	Value	Comment
MBMS User Key	0	User key (PTP)
MBMS Service Key	1	Group key
MBMS Traffic Key	2	Group traffic key

The Key ID length field allows different keys to have different length.

2.3.2 Usage of new general extension payload in MBMS

For example in MSK delivery, the new extension payload includes two Key Type ID sub-payloads where the first sub-payload includes Key Type ‘0’ for MUK (i.e. “outer key”) and the second sub-payload includes Key Type ‘1’ for MSK (i.e. “inner key”). The Data Type field includes ‘0’ indicating pre-shared key message.

3 Reserving UDP port number

A port number in the range 1024-49152 has been requested from IANA for carrying RFC3830 messages over UDP. The numbers in that range do not need an RFC for registration, where as the numbers below 1024 do. The registration has been acknowledged by IANA.

4 Conclusions and proposal

This contribution has described the contents of the internet draft (I-D) for MBMS extensions for RFC 3830 (MIKEY). The I-D concentrates all needed MBMS extensions to a new general extension payload. This means also that the usage of Data Type field in common header and Type field in Key data sub-payload is aligned between MBMS TS and RFC 3830.

It is proposed that SA3 adopts the new general extension payload type presented in the I-D. This means some changes in the current TS and possibly in stage 3, but Ericsson strongly believes that SA3 should take the opportunity to align MBMS extensions with RFC 3830 as much as possible. It is foreseen that this will be more future proof solution and will ease implementation effort.

A CR from Ericsson to this meeting proposes needed changes in TS 33.246.

5 References

[1] IETF RFC 3830 "MIKEY: Multimedia Internet KEYing"

[2] IETF internet draft "The Key ID Information Type for the General Extension Payload in MIKEY” <draft-carrara-newtype-keyid-00.txt>, October 2004

[3] TS 33.246, Security of MBMS

[4] TD S3-040857 “Adding MIKEY payload type identifiers”, SA3#35

Internet Engineering Task Force Carrara, Lehtovirta, Norrman
(Ericsson)

INTERNET-DRAFT
EXPIRES: April 2005 October 2004

The Key ID Information Type for the General Extension Payload in MIKEY

<draft-carrara-newtype-keyid-00.txt>

Status of this memo

Abstract

This memo specifies a new Type (the Key ID Information Type) for the General Extension Payload in the Multimedia Internet KEYing Protocol. This is used in the Multimedia Broadcast/Multicast Service specified in the 3rd Generation Partnership Project.

TABLE OF CONTENTS

1. Introduction

The 3rd Generation Partnership Project (3GPP) is currently involved in the development of a multicast and broadcast service, the Multimedia Broadcast/Multicast Service (MBMS), and its security architecture [MBMS]. This service is specified for 3GPP Release 6.

[MBMS] requires the use of the Multimedia Internet KEYing (MIKEY) Protocol [RFC3830], to convey the keys and related security parameters needed to secure the media that is multicast or broadcast. For the streaming scenario, the security protocol used to protect the media is the Secure Real-time Transport Protocol (SRTP) [RFC3711].

One of the requirements that MBMS puts on security is the possibility to perform frequent updates of the keys. The rationale behind this is that it should be inconvenient for subscribers to publish the decryption keys enabling non-subscribers to view the content. To implement this, MBMS uses a three level key management, to distribute group keys to the clients, and be able to re-key by pushing down a new group key. As illustrated in the section below, MBMS has the need to identify which types of key are involved in the MIKEY message, and their identity.

This memo specifies a new Type for the General Extension Payload in MIKEY, to identify the type and identity of involved keys.

2. The MBMS key management

The key management solution adopted by MBMS uses a three level key management. The keys are used in the way described below. "Clients" refers to the clients who have subscribed to a given multicast/broadcast service.

- - the User Key (MUK), one point-to-point key between the multicast server and each client

- - the Service Key (MSK), one group key between the multicast server and all the clients

- - the Traffic Key (MTK), one group traffic key between the multicast server and all clients.

The Traffic Keys are the keys that are regularly updated.

The point-to-point MUK key (first-level key) is shared between the multicast server and the client via means defined by MBMS [MBMS]. The MUK is used as pre-shared key to run MIKEY with the pre-shared key method [RFC3830], to deliver (point-to-point) the MSK key. The same MSK key is pushed to all the clients, to be used as a (second-level) group key.

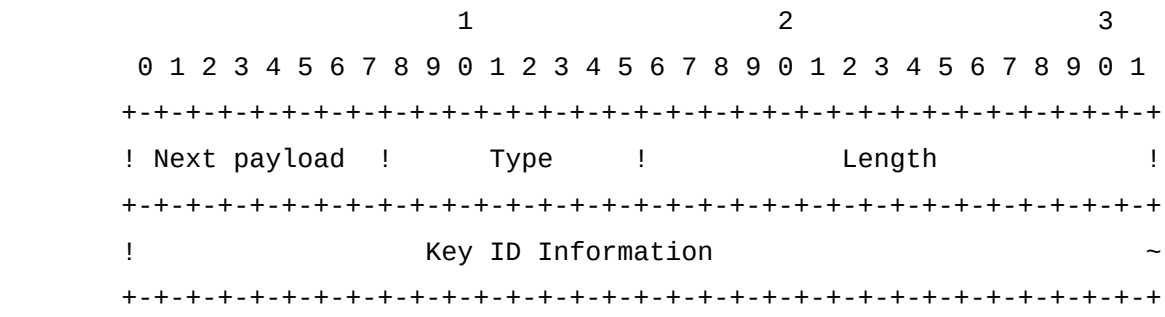
Then, the MSK is used to push to all the clients an MTK key (third-level key), the actual group key that is used for the protection of the media traffic. The MTK is, in other words, the master key for SRTP in the streaming case.

To allow this distribution, an indication of the type and identity of involved keys in the MIKEY message is needed. This indication is carried in a new Type of the General Extension Payload in MIKEY.

3. The Key ID Information Type for the General Extension Payload

The General Extension payload in MIKEY is defined in Section 6.15 of [RFC3830].

The Key ID Information Type (Type 2) formats the General Extension payload as follows:



Next Payload and Length are defined in Section 6.15 of [RFC3830].

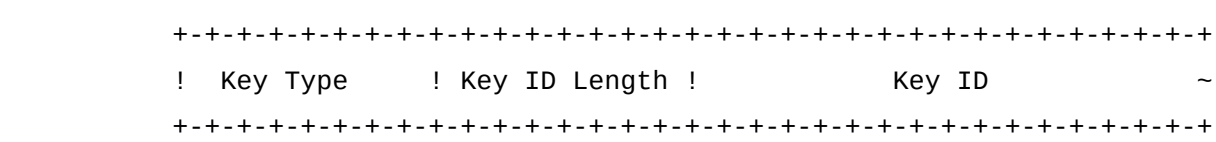
* Type (8 bits): identifies the type of the General Payload [RFC3830]. This memo adds Type 2 to the ones already defined in [RFC3830].

Type	Value	Comments
keyid	2	information on type and identity of keys

Table 1.

* Key ID Information (variable length): the general payload data transporting the type and identifier of a key. This field is formed by Key Type ID sub-payloads as specified below.

The Key Type ID sub-payload is formatted as follows:



* Key Type (8 bits): describes the type of the key. Predefined types are listed in Table 2.

Key Type	Value	Comment
MBMS User Key	0	User key (point-to-point)
MBMS Service Key	1	Group key
MBMS Transport Key	2	Group traffic key

Table 2.

* Key ID Length (8 bits): describes the length of the Key ID field in bytes.

* Key ID (variable length): defines the identity of the key.

Note that there may be more than one Key Type ID sub-payload in an extension, and that the overall length of the Key Identifier ID field cannot exceed 2^16 bytes.

4. Security Considerations

This memo is not foreseen to introduce security implications. For the security considerations of the MIKEY protocol, see [RFC3830].

5. IANA Considerations

A new MIKEY General Extension Payload Type needs to be registered for this purpose. The registered value is requested to be 2 according to Section 3.

The name spaces for the following fields in the General Extensions payload (from Section 3) are requested to be managed by IANA:

* Key Type (Table 2).

6. Acknowledgements

We would like to thank Fredrik Lindholm.

7. Author's Addresses

Questions and comments should be directed to the authors:

Elisabetta Carrara
Ericsson Research
SE-16480 Stockholm Phone: +46 8 50877040
Sweden EMail: elisabetta.carrara@ericsson.com

Vesa Lehtovirta
Ericsson Research
02420 Jorvas Phone: +358 9 2993314

Finland EMail: vesa.lehtovirta@ericsson.com

Karl Norrman
Ericsson Research
SE-16480 Stockholm Phone: +46 8 4044502
Sweden EMail: karl.norrman@ericsson.com

8. References

Normative

[MBMS] 3GPP TS 33.246 V6.0.0 (2004-09), Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security; Security of Multimedia Broadcast/Multicast Service (Release 6)

[RFC3830] Arkko et al., "MIKEY: Multimedia Internet KEYing", RFC 3830, August 2004.

Informative

[RFC3711] Baugher et al., "The Secure Real-time Transport Protocol (SRTP)", RFC3711, March 2004.

Copyright Notice

Disclaimer of Validity

This draft expires in April 2005.

3GPP TSG-SA3 Meeting #36
Shenzhen, China, 23 – 26 November

Tdoc ⌘Att2_S3-040995

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **013** ⌘ **rev** **2** ⌘ 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:	⌘	Implementing general extension payload
Source:	⌘	Ericsson
Work item code:	⌘	MBMS
Date:	⌘	12/11/2004
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:
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:	⌘	A new general extension payload has been introduced in IETF. This CR introduces the payload in the TS.
Summary of change:	⌘	Format of general extnsion payload is introduced. Semantics of Data type field is aligned with MIKEY. Semantics of Type field in Key data subpayload is aligned with MIKEY.
Consequences if not approved:	⌘	The format of new general extension payload type remains unspecified.

Clauses affected:	⌘	2, 6.4.1, 6.4.2, 6.4.4, 6.4.5, 6.4.5.1, 6.4.5.3, 6.4.6.1, 6.4.6.2, 6.5.3, 6.5.4,

Other specs affected:	Y	N			
⌘	X		Other core specifications	⌘	TS 31.102
		X	Test specifications		
		X	O&M Specifications		

Other comments:	⌘	This is rev 2 of CR 013 (S3-040857) that introduced the type value place holders MIKEY fields. This CR takes into account also agreed (and overlapping) changes in 6.4.1 of CR005 (S3-040850) and in 6.5.3 and 6.5.4 of CR008 (S3-040858).

********** 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] IETF internet draft "The Key ID Information Type for the General Extension Payload in MIKEY" <draft-carrara-newtype-keyid-00.txt>

********** NEXT CHANGE**********

6.4.1 General

MIKEY is used to transport the MSKs and MTKs from the BM-SC to the UE. Clauses 6.4.2, 6.4.3, 6.4.4 and 6.4.5 describe how to create the MIKEY messages, while clause 6.4.6 describes the initial processing by the ME on these messages. The final processing is done by the MBMS key Generation and Validation Function (MGV-F) and is described in clause 6.5.

MIKEY shall be used with pre-shared keys as described in RFC 3830 [9].

To keep track of MSKs and MTKs, a new Extension Payload (EXT) [13] is added to MIKEY. The Extension Payload contains the key types and identities of MSKs and the MTKs (see clause 6.3.2 and 6.3.3).

6.4.2 MIKEY common header

~~MIKEY shall be used with pre-shared keys as described in RFC 3830 [9].~~

MSKs shall be carried in MIKEY messages ~~with a Data Type value of 0x07 in the MIKEY common header that signals that the message contains an MBMS MSK. This allows legacy MIKEY implementations to discard the message early in the processing stage~~. The messages are sent point-to-point between the BM-SC and each UE. The messages use the MUK shared between the BM-SC and the UE as the pre-shared secret in MIKEY.

Once the MSK is in place in the UE, the UE can make use of the multicast MTK messages sent by the BM-SC. The MTK is carried in messages conforming to the structure defined by MIKEY and use the MSK as the pre-shared secret. ~~A Data Type value of 0x08 is used in the MIKEY common header to signal that the message contains an MBMS MTK.~~

~~To keep track of MSKs and MTKs, a new Extension Payload (EXT) is added to MIKEY. The Extension contains the identities of MSKs and the MTKs (see clause 6.3.2 and 6.3.3).~~

If the BM-SC requires an ACK for an MSK key update message this is indicated by setting the V-bit in the MIKEY common header. The UE shall then respond with a MIKEY message containing the verification payload. In the case the server does not receive an ACK, normal reliability constructions can be used, e.g., start a timer when the message is sent and then resend the message if no ACK is received before the timer expires.

The CSB ID field of MIKEY common header shall carry the Key Group ID.

******** NEXT CHANGE********

6.4.4 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in RFC 3830 [9] (MIKEY). To be able to keep track of the keys, a ~~new~~ general Extension Payload (EXT) is ~~defined~~ used that conforms to the structure defined in [13] ~~section 6.15 of RFC 3830 [9] (MIKEY)~~.

~~For MBMS the general extension payload (according to table 6.15 of [9]) shall be identified by following value:~~

~~Type~~	~~Value~~	~~Comments~~
~~3GPP MBMS~~	~~x~~	~~3GPP extension payload for MBMS key management~~

~~Editor's Note: The type value will be replaced by an IANA requested value.~~

The types and IDs of the involved keys are kept in the EXT, to enable the UE to look up the type and identity of the key which was used to protect the message, and which key is delivered in the message. This EXT is incorporated in the MIKEY messages (see Figure 6.4).

When a~~n~~ MIKEY message ~~MSK~~ is delivered to a UE, ~~the~~it ~~MIKEY message~~ contains an ~~EXT~~ Extension Payload that ~~holds~~ includes Type field value x.

Editor's Note: The type value will be replaced by an IANA requested value.

The EXT includes two Key Type ID sub-payloads as defined in [13]. These subpayloads identify the outer key ID that is the ID of the key used as pre-shared secret for the key delivery (i.e. an MUK or MSK), and the inner key ID that is transported in the message (i.e. an MSK or MTK). For messages that contain an MSK, the first subpayload includes Key Type and the MUK ID of the MUK used to protect the delivery, and the second subpayload includes the Key Type and MSK ID of the MSK delivered in the message. For messages that contain an MTK, the first subpayload includes Key Type and ~~EXT contains~~ the MSK ID of the MSK used to protect the delivery, and the second subpayload includes the Key Type and MTK ID of the MTK contained in the message. The MSK ID and MTK ID are increased by 1 every time the corresponding key is updated. It is possible that the same MTK is delivered several times in multicast, and the ME can then discard messages related to a key it already has instead of passing them to the MGV-F.

The MGV-F (see clause 6.5) protects itself from a possibly malicious ME by checking the integrity and freshness of the MIKEY message.

The format of the key IDs shall be represented by unsigned integer counters, different from zero. The reason for disallowing zero is that it is reserved for future use. Note that this means that there can only be 2^{n} - 1 different keys in use during the same session, where n is the number of bits in the ID field.

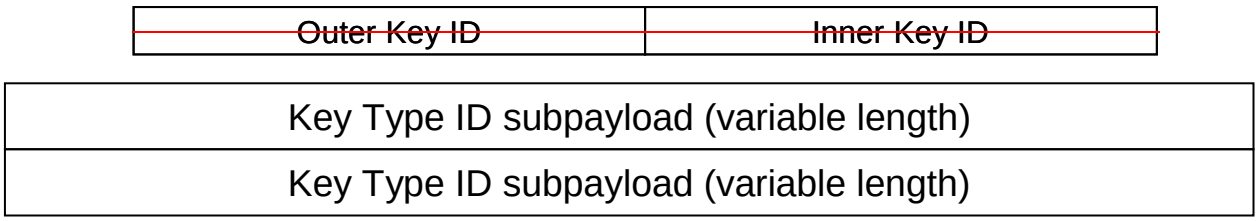


Figure 6.4: Extension payload used with MIKEY

The Inner Key ID is the ID of the key that is transported in the message (i.e. an MSK or MTK). The Outer Key ID is the ID of the key used as pre-shared secret for the key delivery (i.e. an MUK or MSK).

6.4.5 MIKEY message structure

6.4.5.0 MSK and MTK transport identification

For MBMS the MIKEY common header data type field (cf. Table 6.1a of clause 6.1 [9]) identifies the type of key that is transported.

The transport of MSK and MTK transport shall be identified by following values:

Data type	Value	Comment
MSK	x	Transport of MSK encrypted with MUK
MTK	x	Transport of MTK encrypted with MSK

Editor's Note: The type values will be replaced by IANA requested values.

6.4.5.1 MSK message structure

The structure of the MIKEY message carrying a MSK key is depicted in Figure 6.5. The actual key that is delivered is kept in the KEMAC payload. The MIKEY-RAND is used to derive e.g. encryption and authentication keys from the received keys. It is sent only in the initial MSK delivery message. The identity payloads of the initiator's and responder's IDs shall be included in the MSK transport messages. IDi is the ID of the BM-SC and IDr is the ID of the UE. Security Policy (SP) payload includes information for the security protocol such as algorithms to use, key lengths, initial values for algorithms etc. The Key Validity Data subfield is present in the KEMAC payload when MSK is transported but it is not present for MTK transport. The field defines the Key Validity Time for MSK in terms of sequence number interval (i.e. lower limit of MTK ID and upper limit of MTK ID). The lower limit of the interval defines the SEQs to be used by the MGV-F (see clause 6.5).

Editor's Note: The type (URI or NAI) of identity payloads to use are for further study.

Editor's Note: The contents of the Security Policy payload depends on the used security protocols. RFC 3830 [9] (MIKEY) has defined Security Policy payload for SRTP, but for other security protocols there is a need to define new Security Policy payloads. The exact definitions of these are FFS.

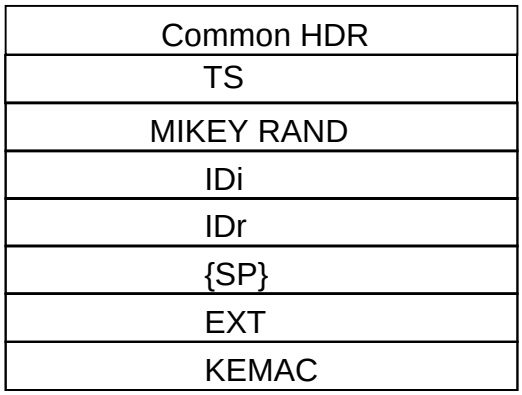


Figure 6.5: The logical structure of the MIKEY message used to deliver MSK.
For use of brackets, cf. section 1.3 of RFC 3830 [9] (MIKEY)

~~6.4.5.1.1 Key Data Sub payloads carried by KEMAC~~

~~For MBMS MSK transport, the Key Data Sub payload (cf. clause 6.13 of [9]) that is carried by the KEMAC payload shall be identified by following value:~~

~~Data type | Value | Comment~~

~~MSK | x | MSK encrypted with MUK~~

~~Editor's Note: The type value will be replaced by an IANA requested value.~~

********** NEXT CHANGE**********

6.4.5.3 MTK message structure

The structure of the MIKEY message carrying a MTK key is depicted in Figure 6.7. The actual key that is delivered is kept in the KEMAC payload. The network identity payloads (IDi) shall be used in MTK transport messages.

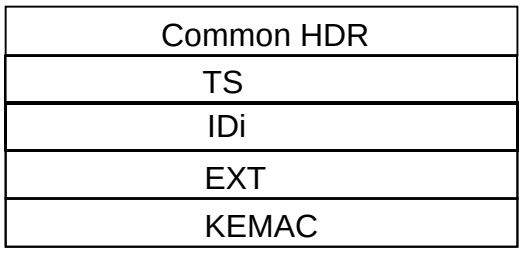


Figure 6.7: The logical structure of the MIKEY message used to deliver MTK

~~6.4.5.3.1 Key Data Sub payloads carried by KEMAC~~

~~For MBMS MTK transport, the Key Data Sub payload (cf. clause 6.13 of [9]) that is carried by the KEMAC payload shall be identified by following value:~~

~~Data type | Value | Comment~~

~~MTK | x | MTK encrypted with MSK~~

~~Editor's Note: The type value will be replaced by an IANA requested value.~~

********** NEXT CHANGE**********

6.4.6 Processing of received messages in the ME

6.4.6.1 MSK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of RFC 3830 [9]).

1. The Extension Payload (~~Data Type field of the common MIKEY header (HDR)~~EXT) is examined, and if it indicates an MSK delivery protected with MUK, the MUK ID is extracted ~~from the Extension Payload~~.
2. The Timestamp Payload is checked, and the message is discarded if the counter is larger or equal to the current MIKEY replay counter associated with the given MUK (the counter value is retrieved from MGV-S). To avoid issues with wrap around of the ID fields "smaller than" should be in the sense of RFC 1982 [10].
3. The Security Policy payload is stored if it was present.
4. The message is transported to MGV-F for further processing, cf clause 6.5.2.
5. The MGV-F replies success or failure.

6.4.6.2 MTK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of RFC 3830 [9]).

1. The Extension Payload (~~Data Type field of the common MIKEY header (HDR)~~ EXT) is examined, and if it indicates an MT~~S~~K delivery protected with MSK, the MSK ID is extracted ~~from the Extension Payload~~.
2. The Timestamp Payload is checked, and the message is discarded if the counter is larger or equal to the current MIKEY replay counter associated with the given MSK (the counter value is retrieved from MGV-S). To avoid issues with wrap around of the ID fields ``smaller than´´ should be in the sense of RFC 1982 [10].
3. If the MTK ID extracted from the Extension payload is less than or equal to the current MTK ID (kept in the ME), the message shall be discarded.
4. The message is transported to MGV-F for further processing, cf 6.5.3.
5. The MGV-F replies success (i.e. sending the MTK) or failure.

******** NEXT CHANGE********

6.5.3 MSK processing~~validation and derivation~~

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the ~~Data Type field in the common header~~EXT. If the key in the message is an MSK protected by MUK, MGV-F retrieves the MUK with the ID given by the Extension payload.

~~The MAC in the KEMAC payload is verified using MUK_I, and the message is discarded if verification fails. If the MAC verification is successful the MUK_C is used to decrypt the Key Data sub-payload, and the MSK can be installed in the MGV-S. The MSK is used as pre-shared secret together with the MIKEY-RAND and the Key Group ID from the MIKEY message to derive (as specified in section 4.1.4 of RFC 3830 [9]) encryption and integrity keys (MSK_I and MSK_C).~~ The integrity of the message is validated and the MSK is extracted from the KEMAC payload as described in Section 5 of [9] if the validation is successful. The Key Validity data is extracted from the message and stored (in the form of MTK ID interval). The lower limit of the interval defines the SEQs.

NOTE: The MSK is not necessarily updated in the message, since a MSK transport message can be sent e.g. to update the Key Validity data.

If messageMAC verificvalidation is successful, then the MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MUK ID.

6.5.4 MTK processingvalidation and derivation

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the Data Type field in the common headerEXT. If the key inside the message is an MTK protected by MSK, MGV-F retrieves the MSK with the ID given by the Extension payload.

It is assumed that the MBMS service specific data, MSK and the sequence number SEQs, have been stored within a secure storage (MGV-S). Both MSK and SEQs were transferred to the MGV-S with the execution of the MSK update procedures. The initial value of SEQs is determined by the service provider.

The MGV-F shall only calculate and deliver the MBMS Traffic Keys (MTK) to the ME if the ptm-key information is deemed to be fresh.

The MGV-F shall compare the received SEQp, i.e. MTK ID from the MIKEY message with the stored SEQs. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME. If SEQp is greater than SEQs then the MGV-F shall verify the integrity of the MIKEY message according to RFC 3830 [9]. calculate the MAC as defined in RFC 3830 [9] using the received MIKEY message and MSK as input. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message. If the MAC verification is unsuccessful, then the MGV-F will indicate a failure to the ME. If the MAC verification is successful, then the MGV-F shall update SEQs with SEQp value and extract the start the generation of MTK from the message. The MGV-F then provides the MTK to the ME.

The MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MSK ID.

NOTE: MIKEY includes functionality to derive further keys from MTK if needed by the security protocol. The key derivation is defined in section 4.1.3 of RFC 3830 [9] (MIKEY).].