3GPP TSG SA WG3 Security — SA3#37 **S3-050080**
February 21-25, 2005
Sophia Antipolis, France

Source: Ericsson

Title: Status of MIKEY related IETF work

Agenda item: MBMS

Document for: Discussion/Decision

1 Introduction

This contribution reports the status of MIKEY related IETF activities.

2 Discussion

In the last SA3 meeting Ericsson got the action to add the MBMS extensions MIKEY draft [2] to 3GPP- IETF dependency list. The draft has been added to the list.

The internet draft has been adopted as IETF Work Group draft. Therefore its name has changed to [2]. The category of the draft (informational or standards track) will be decided by the IETF MSEC WG.

The draft was updated to include the Key Domain ID according to SA3 decision in S3-04xxxx.

The latest version (draft-ietf-msec-newtype-keyid-01.txt) of the draft includes also a new value for “CS ID map type” field in the common header. The new value is needed to allow also security protocols that don’t need to send any security policy via MIKEY protocol [3].

Due to Rel-6 timescales and maturity of the draft, Ericsson intends to send the draft to WG last call in the near future. The WG last call , when announced, will take two weeks. Ericsson will inform SA3 on the last call time table in SA3 mailing list and would like to invite SA3 companies to provide comments to the draft before the last call deadline . Ericsson volunteers to forward possible SA3 comments to IETF MSEC group.

UDP/TCP port number has been assigned to MIKEY by IANA. The number is 2269.

3 Conclusion & Proposal

This contribution has given the status of MIKEY related IETF work. Needed changes have been implemented in the accompanying CR to TS 33.246. The draft is also attached for information.

4 References

[1] 3GPP TS 33.246: " Security; Security of Multimedia Broadcast/Multicast Service"

[2] Internet Draft: “The Key ID Information Type for the General Extension Payload in MIKEY ", draft-ietf-msec-newtype-keyid-00.txt

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

3GPP TSG-SA WG3 Meeting S3#37
Sophia, France, 21-25 February, 2005

Tdoc ⌘Att1_S3-050080

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**043**	⌘**rev**	**-**	⌘	Current version:	**6.1.0** ⌘

*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:	⌘	Alignment according to MIKEY related IETF work		
Source:	⌘	Ericsson		
Work item code:	⌘	MBMS	***Date:*** ⌘	14/2/2005
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:	⌘	MIKEY IETF draft has been updated.
Summary of change:	⌘	Removed some editor's notes about pending IETF work and added UDP port number for MIKEY.
Consequences if not approved:	⌘	TS is not aligned with IETF draft

Clauses affected:	⌘	2, 6.3.3.2.2, 6.4.1, 6.4.2, 6.4.4				
		Y	N			
Other specs Affected:	⌘		N	Other core specifications	⌘	
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

******* 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] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service; Protocols and Codecs".

[14] 3GPP TS 33.210: "Network domain security; IP network layer security".

[15] OMA-DRM-DCF-v2_0: "OMA DRM Content Format", www.openmobilealliance.org

[16] IETF internet draft: "The Key ID Information Type for the General Extension Payload in MIKEY" <draft-~~carrara~~msec-newtype-keyid-0~~0~~1.txt>.

[xx] Port numbers at IANA, http://www.iana.org/assignments/port-numbers

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

6.3.3.2.~~1~~2 MTK delivery in streaming

MIKEY messages transporting MTKs shall be sent using the same IP address as the RTP traffic. MIKEY messages shall be transported to UDP port number specified for MIKEY.

~~Editor's Note: The UDP port number needs to be specified for MIKEY.~~

***** 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]. The UDP port number for MIKEY is 2269 [xx]

To keep track of MSKs and MTKs, a new Extension Payload (EXT) [16] is added to MIKEY. The Extension Payload can contain the key types and identities of MSK and the MTK and Key Domain ID (see clauses 6.3.2 and 6.3.3).

6.4.2 MIKEY common header

MSKs shall be carried in MIKEY messages. 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.

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 is not used.

***** 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 key that is derived in the message, a general Extension Payload (EXT) with Type field value x is used that conforms to the structure defined in reference [16].

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

The EXT includes a Key Domain ID and one or two Key Type ID sub-payloads depending on the message. These are used as follows.

For MSK delivery the EXT includes the Key Domain ID and a Key Type ID sub-payload. The Key Domain ID has the value as specified in clause 6.3.2.1. The Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MSK ID, see figure 6.4a. The key that is used to protect the message, i.e. MUK, is identified as specified in clause 6.1.

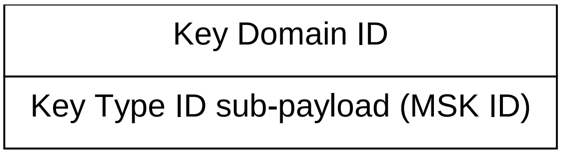
For MTK delivery the EXT includes the Key Domain ID and two Key Type ID sub-payloads. The Key Domain ID has the value as specified in clause 6.3.2.1. The first Key Type ID sub-payload includes the type and ID of the key that is used to protect the message, i.e. the MSK ID, and the second Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MTK ID, see figure 6.4b.

~~Editor's Note: The Key Domain ID needs to be added to [16]. It may need an extension payload type of its own.~~

See. clauses 6.3.2.1 and 6.3.3.1 for definition of MSK ID and MTK ID. The MTK ID is increased 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.

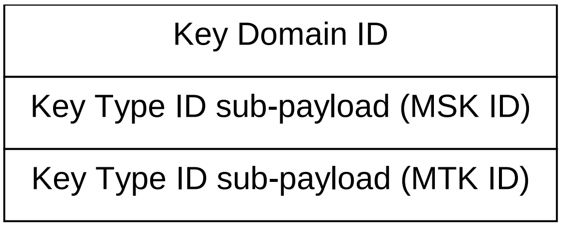
The format of the key IDs shall be represented by unsigned integers, different from zero. The reason for disallowing zero is that it is reserved for future use. Note that this means that there can only be 2^n - 1 different keys in use during the same session, where n is the number of bits in the ID field.



Key Domain ID

Key Type ID sub-payload (MSK ID)

Figure 6.4a: Extension payload used with MIKEY MSK message



Key Domain ID

Key Type ID sub-payload (MSK ID)

Key Type ID sub-payload (MTK ID)

Figure 6.b: Extension payload used with MIKEY MTK message

Internet Engineering Task Force

Carrara, Lehtovirta, Norrman
(Ericsson)

INTERNET-DRAFT
EXPIRES: August 2005
February 2005

The Key ID Information Type for the General Extension Payload in MIKEY
<draft-ietf-msec-newtype-keyid-01.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, e.g., 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].

[MBMS] requires the use of the Multimedia Internet KEYing (MIKEY) Protocol [RFC3830], to convey the keys and related security parameters needed to secure the multimedia that is multicast or broadcast.

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. Rationale

An application where this extension is used is 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 MBMS User Key (MUK), point-to-point key between the multicast server and each client

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

- the MBMS Traffic Key (MTK), 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. For example, the MTK could be the master key for SRTP [3711] in the streaming case.

A Key Domain identifier defines the domain where the group keys are valid or applicable. For example it may define a specific service provider.

To allow the key distribution described above, 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.

It is necessary to specify what Crypto Session ID map type is associated with a given key. There are cases, for example the download case in MBMS, where the required parameters are signalled in-band. This implies that a CS ID map type needs to be registered to the "empty map" as defined in Table 3, which is to be used when the map/policy information is conveyed outside of 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 3) formats the General Extension payload as follows:

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
! Next payload  !      Type     !            Length             !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                  Key ID Information                           ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 3 to the ones already defined in [RFC3830].

Type	Value	Comments
Key ID	3	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 ID Type sub-payloads as specified below.

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

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!  Key ID Type  ! Key ID Length !            Key ID             ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

Key ID Type	Value	Comment
MBMS Key Domain ID	0	ID of the group key domain
MBMS Service Key ID	1	ID of the group key
MBMS Transport Key ID	2	ID of the 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 ID Type sub-payload in an extension, and that the overall length (i.e., the sum of lengths of all Key ID Type sub-payloads) of the Key ID information field cannot exceed 2^16 bytes. Applications using this general extension payload have to define the semantics and usage of the Key ID Type sub-payloads.

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

When the security policy information is conveyed outside of MIKEY, the CS ID map type is set to value defined in Table 3 to indicate "empty map".

CS ID map type	Value	Comments
Empty map	0	Used when the map/policy information is conveyed outside of MIKEY

Table 3.

5. Security Considerations

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

6. IANA Considerations

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

The name spaces for the following fields in the General Extensions payload (from Sections 3 and 4) are requested to be managed by IANA:

* Key ID Type (Table 2).

* New value for CS ID map type (Table 3).

7. Acknowledgements

We would like to thank Fredrik Lindholm.

8. 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

9. References

Normative

[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.

[MBMS] 3GPP TS 33.246, Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security; Security of Multimedia Broadcast/Multicast Service.

Copyright Notice

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

This draft expires in August 2005.