

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

By submitting this Internet-Draft, the authors certify that any applicable patent or other IPR claims of which I am (we are) aware have been disclosed, and any of which I (we) become aware will be disclosed, in accordance with [RFC 3668](#) ([BCP 79](#)).

By submitting this Internet-Draft, the authors accept the provisions of [Section 3 of RFC 3667](#) ([BCP 78](#)).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or cite them other than as "work in progress".

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

This document is an individual submission to the IETF. Comments should be directed to the authors.

## 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.

INTERNET-DRAFT

newtype-keyid

October, 2004

## TABLE OF CONTENTS

<a href="#">1.</a>	<a href="#">Introduction.....</a>	<a href="#">2</a>
<a href="#">2.</a>	<a href="#">The MBMS key management.....</a>	<a href="#">2</a>
<a href="#">3.</a>	<a href="#">The Key ID Information Type for the General Extension Payload..</a>	<a href="#">3</a>
<a href="#">4.</a>	<a href="#">Security Considerations.....</a>	<a href="#">5</a>
<a href="#">5.</a>	<a href="#">IANA Considerations.....</a>	<a href="#">5</a>
<a href="#">6.</a>	<a href="#">Acknowledgements.....</a>	<a href="#">5</a>
<a href="#">7.</a>	<a href="#">Author's Addresses.....</a>	<a href="#">5</a>
<a href="#">8.</a>	<a href="#">References.....</a>	<a href="#">6</a>

## [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:

```

          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 \[RFC3830\]](#).

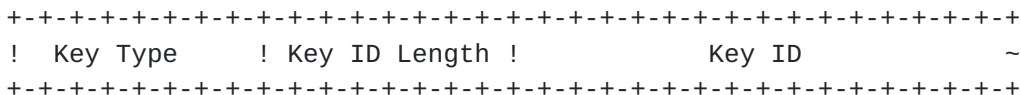
\* Type (8 bits): identifies the type of the General Payload [RFC3830]. This memo adds Type 2 to the ones already defined in [RFC3830].

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](mailto:elisabetta.carrara@ericsson.com)

Vesa Lehtovirta  
Ericsson Research  
02420 Jorvas              Phone: +358 9 2993314  
Finland                      EMail: [vesa.lehtovirta@ericsson.com](mailto:vesa.lehtovirta@ericsson.com)



Karl Norrman  
Ericsson Research  
SE-16480 Stockholm  
Sweden

Phone: +46 8 4044502  
EMail: karl.norrman@ericsson.com

Carrara, Norrman

[Page 5]

## **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

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

### 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 April 2005.

Carrara, Norrman

[Page 6]