The Key ID Information Type for the General Extension Payload in MIKEY
<draft-ietf-msec-newtype-keyid-01.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, e.g., the Multimedia Broadcast/Multicast Service specified in the 3rd Generation Partnership Project.
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:

```
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].

```
<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key ID</td>
<td>3</td>
<td>information on type and identity of keys</td>
</tr>
</tbody>
</table>
```

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.

```
<table>
<thead>
<tr>
<th>Key ID Type</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBMS Key Domain ID</td>
<td>0</td>
<td>ID of the group key domain</td>
</tr>
<tr>
<td>MBMS Service Key ID</td>
<td>1</td>
<td>ID of the group key</td>
</tr>
<tr>
<td>MBMS Transport Key ID</td>
<td>2</td>
<td>ID of the group traffic key</td>
</tr>
</tbody>
</table>
```

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".

<table>
<thead>
<tr>
<th>CS ID map type</th>
<th>Value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empty map</td>
<td>0</td>
<td>Used when the map/policy information is conveyed outside of MIKEY</td>
</tr>
</tbody>
</table>

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


Informative


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 August 2005.