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.

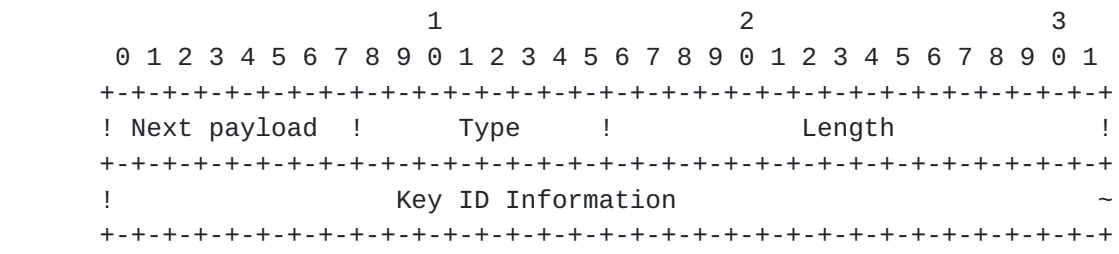
Then, the MSK is used to push to all the clients an MTK key (third-level key), the actual group key that is used for the protection of the media traffic. The MTK is, in other words, the master key for SRTP in the streaming case.

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].

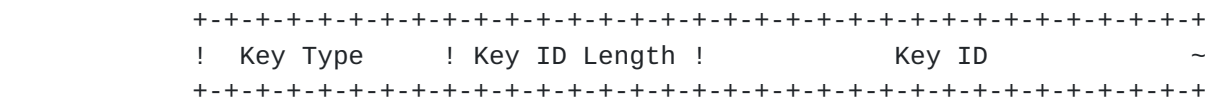
* Type (8 bits): identifies the type of the General Payload [RFC3830]. This memo adds Type 2 to the ones already defined in [RFC3830].

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.

This draft expires in April 2005.