Network Working Group
Request for Comments: 4909
Category: Informational

L. Dondeti, Ed.
QUALCOMM, Inc.
D. Castleford
France Telecom
F. Hartung
Ericsson Research

June 2007

Multimedia Internet KEYing (MIKEY) General Extension Payload for Open Mobile Alliance BCAST LTKM/STKM Transport

Status of This Memo

Copyright Notice

Abstract

This document specifies a new Multimedia Internet KEYing (MIKEY) General Extension payload (RFC 3830) to transport the short-term key message (STKM) and long-term key message (LTKM) payloads defined in the Open Mobile Alliance's (OMA) Browser and Content (BAC) Broadcast (BCAST) group's Service and Content protection specification.

Table of Contents

1. Introduction

The Multimedia Internet Keying (MIKEY) protocol specification [1] defines a General Extension payload to allow possible extensions to MIKEY without having to allocate a new payload type. The General Extension payload can be used in any MIKEY message and is part of the authenticated/signed data part. There is an 8-bit type field in that payload. The type code assignment is IANA-managed, and RFC 3830 requires IETF consensus for assignments from the public range of 0-240.

The Open Mobile Alliance's (OMA) Browser and Content (BAC) Broadcast (BCAST) group's Service and Content Protection specification [2] specifies the use of a short-term key message (STKM) and a long-term key message (LTKM) that carry attributes related to Service and Content protection. Note that any keys associated with the attributes are part of the MIKEY KEMAC payload. This document specifies the use of the General Extension payload of MIKEY to carry the LTKMs or STKMs.

RFC 3830 [1], the MIKEY General Extension payload defined in [3], and the 3rd Generation Partnership Project (3GPP)'s Multimedia Broadcast/ Multicast Service (MBMS) document [4] specify the transport of MIKEY messages via unicast or broadcast and the OMA specifications use either for transport of MIKEY messages.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [5].

OMA BCAST STKM/LTKM MIKEY General Extension: We refer to the General Extension type -- 5 -- as the OMA BCAST STKM/LTKM MIKEY General Extension .

3. MIKEY General Extension for OMA BCAST Usage

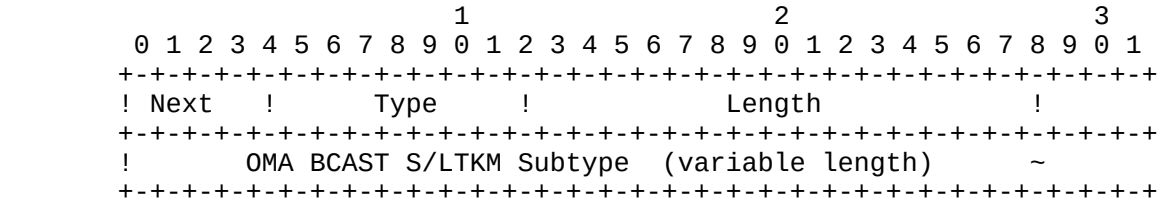

Figure 1: OMA BCAST MIKEY General Extension

Section 6.1 of RFC 3830 specifies the first three fields of the General Extension Payload and defines a variable length Data field. This document specifies the use of Type 5 for OMA BCAST Service and Content Protection using the Smartcard Profile. The contents of the variable length data field are defined below.

Subtype: 8 bits. This field indicates the type of the OMA BCAST payload. In this specification, only two values are specified: LTKM (1), and STKM (2).

Subtype Specific Data: Variable length. The contents of this field are defined in Section 6 of the OMA BCAST Service and Content Protection specification [2].

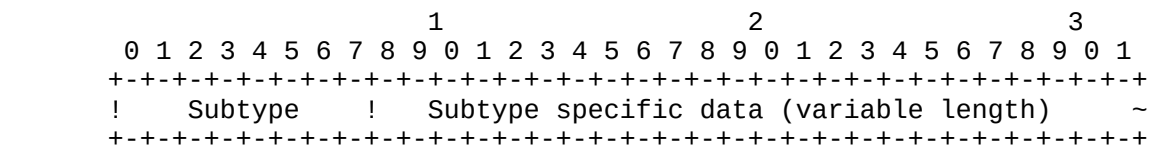

Figure 2: STKM/LTKM Subtype Payload

4. Interoperability Considerations

This document specifies the use of MIKEY General Extension Payload Type 5 and a couple of subtype values (1 and 2), one each for OMA BCAST Service and Content protection's STKM and LTKM payloads. Interoperability considerations span several standards bodies, with OMA BCAST 1.0 enabler compliance being the key aspect; as such, it is up to the OMA test planning to verify the interoperability and compliance of OMA BCAST 1.0 implementations. This payload type assignment does not change MIKEY beyond RFC 3830 [1] and RFC 4563 [3].

5. Security Considerations

According to RFC 3830, the general extension payload can be used in any MIKEY message and is part of the authenticated/signed data part. The parameters proposed to be included in the OMA BCAST MIKEY General Extension payload (listed in Section 3) need only to be integrity protected, which is already allowed by the MIKEY specification. The OMA BCAST MIKEY General Extension Payload SHALL be integrity protected. Furthermore, keys or any parameters that require confidentiality MUST NOT be included in the General Extension Payload. If keys or other confidential data are to be transported via the General Extension Payload, such data MUST be encrypted and encapsulated independently. Finally, note that MIKEY already provides replay protection and that protection covers the General Extension Payload also.

6. IANA Considerations

IANA has allocated a new General Extension Type from the "General Extensions payload name spaces" in the IANA registry at http://www.iana.org/assignments/mikey-payloads for use by OMA BCAST. Furthermore, IANA maintains a list of corresponding subtypes (0-255) as follows:

0 ... Reserved

1 ... LTKM

2 ... STKM

3 ... 191 (maintained by IANA and assigned by IETF Review [6])

192 ... 255 (Private use)

7. Acknowledgments

Many thanks to Jari Arkko, Piron Laurent, and Steffen Fries for their reviews and suggestions for improvement.

8. References

8.1. Normative References

[1] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, August 2004.

[2] Open Mobile Alliance, "Service and Content Protection for Mobile Broadcast Services", OMA TS-BCAST_SvcCntProtection-V1_0-20070529-C, 2007, <http://www.openmobilealliance.org/release_program/bcast_v1_0.html>.

[3] Carrara, E., Lehtovirta, V., and K. Norrman, "The Key ID Information Type for the General Extension Payload in Multimedia Internet KEYing (MIKEY)", RFC 4563, June 2006.

[4] 3GPP, "3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)", 3GPP TS 33.246 6.6.0, March 2006.

[5] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2. Informative References

[6] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", Work in Progress, March 2007.

Authors' Addresses

Lakshminath Dondeti (editor)
QUALCOMM, Inc.
5775 Morehouse Dr
San Diego, CA
USA

Phone: +1 858-845-1267
EMail: ldondeti@qualcomm.com

David Castleford
France Telecom
4, rue du Clos Courtel
35512 Cesson Sevigne Cedex,
France

Phone: + 33 (0)2 99 12 49 27
EMail: david.castleford@orange-ftgroup.com

Frank Hartung
Ericsson Research
Ericsson Allee 1
52134 Herzogenrath,
Germany

Phone: +49 2407 575389
EMail: frank.hartung@ericsson.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.