Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 10, 2007

L. Dondeti, Ed.
QUALCOMM, Inc.
D. Castleford
Orange FT
F. Hartung
Ericsson Research
February 6, 2007

MIKEY General Extension Payload for OMA BCAST LTKM/STKM Transport
draft-dondeti-msec-mikey-genext-oma-04

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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 to 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 Internet-Draft will expire on August 10, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document specifies a new MIKEY General Extension payload [1] 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 3
2. Terminology 3
3. MIKEY General Extension for OMA BCAST Usage 3
4. Interoperability considerations 4
5. Security Considerations 5
6. IANA Considerations 5
7. Acknowledgments 5
8. References 5
8.1. Normative References 5
8.2. Informative References 6
Authors' Addresses 6
Intellectual Property and Copyright Statements 8

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 and 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, the MIKEY General Extension payload defined in [3] along with the 3rd Generation Partnership Project (3GPP)'s Multimedia Broadcast/Multicast Service (MBMS) [4] document 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 -- value, to be assigned by IANA -- as the OMA BCAST STKM/LTKM MIKEY General Extension .

3. MIKEY General Extension for OMA BCAST Usage

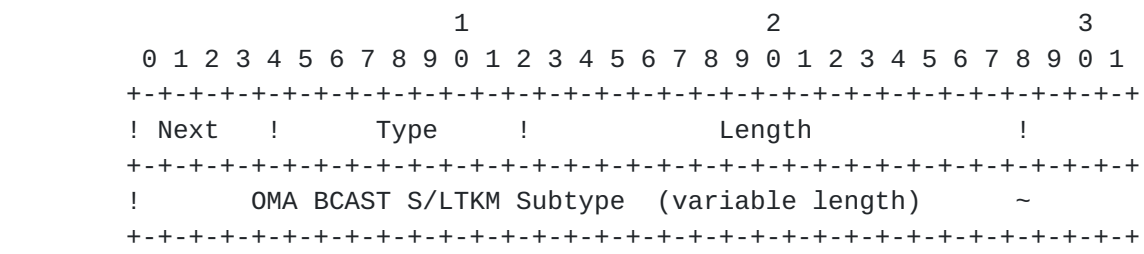

Figure 1: OMA BCAST MIKEY General Extension

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 XX [To be filled in by the RFC Editor after IANA assignment] for OMA BCAST Service and Content Protection using the Smartcard Profile. The contents of the variable length data field are defined below.

Sub Type: 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).

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

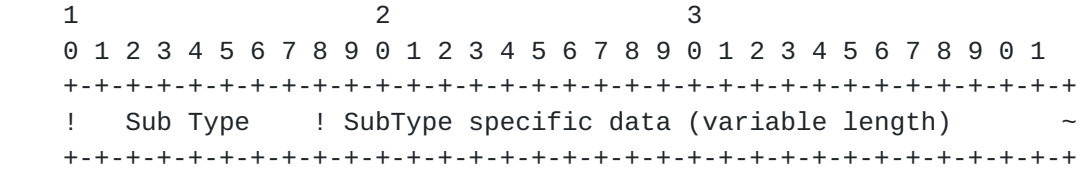

Figure 2: STKM/LTKM Subtype Payload

4. Interoperability considerations

This document specifies the use of MIKEY General Extension Payload Type XX [to be assigned by IANA based on IETF review] 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 and [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 is requested to allocate 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 is requested to maintain 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_0-20060412-D, 2006.

[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", draft-narten-iana-considerations-rfc2434bis-05 (work in progress), September 2006.

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
Orange FT
4, rue du Clos Courtel
35512 Cesson Sevigne Cedex,
France

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

Frank Hartung
Ericsson Research
Ericsson Allee 1
52134 Herzogenrath,
Germany

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

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

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.

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, THE IETF TRUST 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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).