

Network Working Group  
Internet-Draft  
Obsoletes: [4909](#) (if approved)  
Intended status: Informational  
Expires: April 27, 2009

A. Jerichow, Ed.  
Nokia Siemens Networks  
L. Piron  
Nagravision S.A.  
October 24, 2008

MIKEY General Extension Payload for OMA BCAST 1.0  
draft-jerichow-msec-mikey-genext-oma-00

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 April 27, 2009.

Abstract

This document extends the General Extension Payload for OMA BCAST usage defined in [RFC 4909](#) [1]. It adds necessary support for the newly specified management data as defined in the Open Mobile Alliance's (OMA) Broadcast (BCAST) group's Service and Content protection specification [2].

Internet-Draft

OMA BCAST MIKEY GenExt

October 2008

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">3.</a>	MIKEY General Extension for OMA BCAST Usage . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Interoperability considerations . . . . .	<a href="#">5</a>
<a href="#">5.</a>	Security Considerations . . . . .	<a href="#">5</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">5</a>
<a href="#">7.</a>	Changes since <a href="#">RFC 4909</a> . . . . .	<a href="#">6</a>
<a href="#">8.</a>	Acknowledgments . . . . .	<a href="#">6</a>
<a href="#">9.</a>	Normative References . . . . .	<a href="#">6</a>
	Authors' Addresses . . . . .	<a href="#">7</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">8</a>

## 1. Introduction

The Multimedia Internet Keying (MIKEY) protocol specification ([RFC 3830](#) [3]) 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) Broadcast (BCAST) group's Service and Content Protection specification [2] specifies the use of a short-term key message (STKM), a long-term key message (LTKM), a LTKM reporting message, as well as a parental control message that carry attributes related to Service and Content protection. Note that any keys associated with the attributes, such as the Parental Control Pincode if present, are part of the MIKEY KEMAC payload.

This document specifies the use of the General Extension payload of MIKEY to carry the messages mentioned above, as well as protection of the credentials using mechanisms supported by MIKEY with modifications in [3].

[RFC 3830](#) [3], the MIKEY General Extension payload defined in [RFC 4563](#) [4], and the 3rd Generation Partnership Project (3GPP)'s Multimedia Broadcast/ Multicast Service (MBMS) document [5] 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](#) [6].

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

3. MIKEY General Extension for OMA BCAST Usage

[Section 6.1 of RFC 3830](#) [3] specifies the first three fields of the General Extension Payload and defines a variable length Data field.

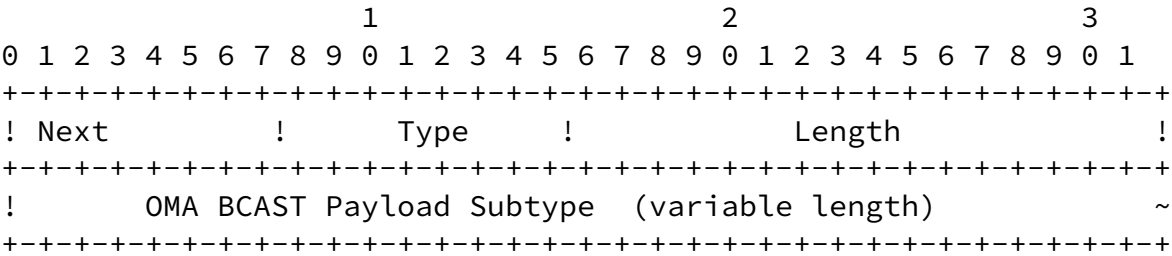


Figure 1: OMA BCAST MIKEY General Extension

This document specifies the use of Type 5 for OMA BCAST Service and Content Protection using the Smartcard Profile.

Type	Value	Comments
OMA BCAST	5	information on type and identity of messages

Figure 2: Definition of the New General Extension Payload

The contents of the variable length data field are defined below.

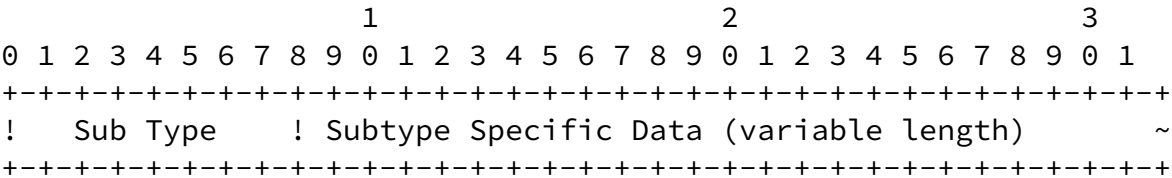


Figure 3: STKM/LTKM/LTKM Reporting/Parental Control Subtype Payload

Sub Type: 8 bits. This field indicates the type of the OMA BCAST payload. In this specification, four values are specified: LTKM (1), STKM (2), LTKM Reporting (TBD1), and Parental Control (TBD2).

Sub Type Specific Data: Variable length.

OMA BCAST Type	Value	Comment
LTKM	1	Long Term Key Message
STKM	2	Short Term Key Message
LTKM Reporting	TBD1	LTKM Reporting Message
Parental Control	TBD2	Parental Control Message

Figure 4: Subtype definitions for OMA BCAST messages

The contents of the OMA BCAST payload field are defined in [Section 6](#) of the OMA BCAST Service and Content Protection specification [\[2\]](#).

#### [4.](#) Interoperability considerations

This document specifies the use of MIKEY General Extension Payload Type 5 and four subtype values (1, 2, TBD1 and TBD2), 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](#) [\[3\]](#) and [RFC 4563](#) [\[4\]](#).

#### [5.](#) Security Considerations

According to [RFC 3830](#) [\[3\]](#), 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 also the General Extension Payload.

## [6.](#) IANA Considerations

IANA has allocated an OMA BCAST MIKEY General Extension Type --5-- from the "General Extensions payload name space" in the IANA registry at <http://www.iana.org/assignments/mikey-payloads> for use by OMA BCAST as requested by [RFC 4909](#) [[1](#)]. Furthermore, IANA has created a name space for the OMA BCAST payload subtype values defined in [[1](#)] and has assigned the following subtype values from this name space: LTKM (1), STKM (2).

IANA is requested to allocate two new subtypes from the OMA BCAST payload subtype name space, referenced above, in the IANA registry at <http://www.iana.org/assignments/mikey-payloads>.

The requested subtypes are as follows:

Subtype Name: LTKM Reporting

Value: TBD1

Suggested value: 3

and

Subtype Name: Parental Control

Value: TBD2

Suggested value: 4

Note to Editor: Please replace all TBD1 and TBD2 in this specification with the values assigned by IANA.

## 7. Changes since [RFC 4909](#)

OMA BCAST Service and Content Protection specification [2] contains messages that were created since [RFC 4909](#) was written. This document only adds the necessary assignments to support these new messages. No modifications are made on values assigned by [RFC 4909](#) [1].

## 8. Acknowledgments

Many thanks to the authors of [RFC 4909](#) [1] for allowing to update their RFC.

## 9. Normative References

- [1] "Multimedia Internet KEYing (MIKEY) General Extension", [RFC 4909](#), June 2007.
- [2] Open Mobile Alliance, "Service and Content Protection for Mobile Broadcast Services", OMA OMA-TS-BCAST\_SvcCntProtection-V1\_0-20081015-D, 2008.
- [3] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", [RFC 3830](#), August 2004.
- [4] 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.

- [5] 3GPP, "3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)", 3GPP TS 33.246 6.6.0, March 2006.
- [6] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

## Authors' Addresses

Anja Jerichow (editor)  
Nokia Siemens Networks  
Martinstr. 76  
81541 Munich  
Germany

Phone: +49 89 636-45868  
Email: [anja.jerichow@nsn.com](mailto:anja.jerichow@nsn.com)

Laurent Piron  
Nagravision S.A.  
Case Postale 134  
1033 Cheseaux  
Switzerland

Phone: +41 21 732 05 37  
Email: [laurent.piron@nagravision.com](mailto:laurent.piron@nagravision.com)



Copyright (C) The IETF Trust (2008).

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](mailto:ietf-ipr@ietf.org).