

Network Working Group
Internet-Draft
Expires: October 30, 2006

L. Dondeti, Ed.
QUALCOMM, Inc.
D. Castleford
Orange, FTR&D
April 28, 2006

OMA BCAST MIKEY General Extension Payload Specification
draft-dondeti-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/lid-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 October 30, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document specifies a new general extension payload type for use in the Open Mobile Alliance's (OMA) Browser and Content (BAC) Broadcast (BCAST) group. OMA BCAST's service and content protection specification uses short term key message (STKM) and long term key message (LTKM) payloads that in certain broadcast distribution systems (BDS) are carried in the IETF MIKEY protocol [[1](#)]. A new MIKEY general extension payload specified in this document will be

Internet-Draft OMA BCAST MIKEY General Extension Payload

April 2006

used for that purpose.

Table of Contents

1.	Introduction	3
2.	Terminology	3
3.	MIKEY General Extension Payload for OMA BCAST Usage	3
4.	Interoperability considerations	4
5.	Security Considerations	5
6.	IANA Considerations	5
7.	Normative References	5
	Authors' Addresses	6
	Intellectual Property and Copyright Statements	7

[1.](#) Introduction

The MIKEY specification [[1](#)] defines a General extensions payload to allow possible extensions to MIKEY without defining a new payload. 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 OMA BCAST Service and Content Protection specification [[2](#)] specifies the use of an STKM and an LTKM that carries attributes related to service and content protection (any keys associated with the attributes are part of the MIKEY message). The STKM or the LTKM is to be carried in a MIKEY message in the context of the 3rd Generation Partnership Project (3GPP)'s Multimedia Broadcast/Multicast Service (MBMS) BDS. This document specifies the use of the general extension payload of MIKEY's general extension payload to carry the LTKMs or STKMs.

The MIKEY general extension payload specified in [[3](#)] along with the MBMS [[4](#)] specification specifies 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 General Extension payload: We refer to the general extension payload type -- value, to be assigned by IANA -- as the OMA GenExt payload.

3. MIKEY General Extension Payload for OMA BCAST Usage

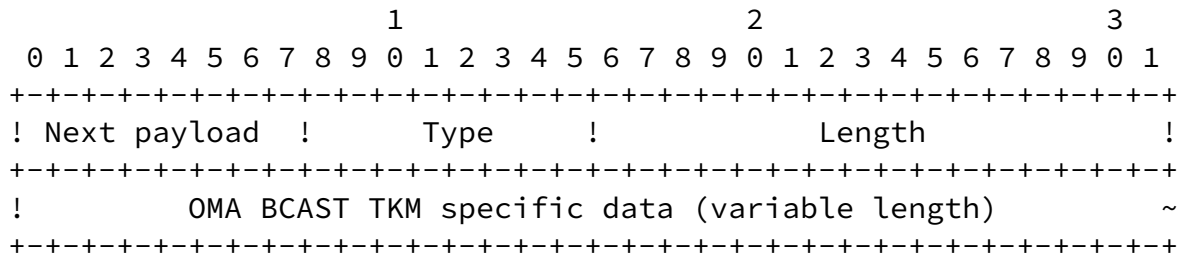


Figure 1: OMA General Extension Payload

The intent is to define a fixed length TKM type variable as part of the OMA BCAST TKM SpecificData and use that to differentiate between STKMs and LTKMs.

The only new field introduced from the IETF perspective is the OMA BCAST TKM specific data (variable length):

OMA BCAST STKM contains the following fields:

- protocol_version
- protection_after_reception
- reserved_for_future_use
- access_criteria_flag
- traffic_protection_protocol
- traffic_authentication_flag
- reserved_for_future_use
- traffic_key_lifetime

If access_criteria_flag is TRUE the following fields are present

reserved_for_future_use

number_of_access_criteria_descriptors

access_criteria_descriptors

OMA BCAST LTKM contains the following fields:

TerminalBindingKeyID

RightsIssuerURI

[4.](#) Interoperability considerations

This document requests a MIKEY [[1](#)] General Extension Payload Type number from IANA through IETF review. The payload defined is relevant to the 3GPP MBMS adaptation of the OMA BCAST 1.0 specification. Interoperability considerations span at least 3 SDOs

Dondeti & Castleford

Expires October 30, 2006

[Page 4]

Internet-Draft OMA BCAST MIKEY General Extension Payload

April 2006

and as such it is up to the OMA test planning to verify the interoperability of the MBMS adaptation of OMA BCAST 1.0. 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's 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. Note that MIKEY already provides replay protection and that protection covers the General Extension Payload also.

[6.](#) IANA Considerations

Please provide the next available number from the "General Extensions payload name spaces" in the IANA registry at <http://www.iana.org/assignments/mikey-payloads> for use by OMA BCAST GenExt payload.

7. 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., "The Key ID Information Type for the General Extension Payload in MIKEY", [draft-ietf-msec-newtype-keyid-05](#) (work in progress), March 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.

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, FTR&D
4, rue du Clos Courtel

35512 Cesson Sevigne Cedex,
France

Phone: + 33 (0)2 99 12 49 27

Email: david.castleford@francetelecom.com

Intellectual Property Statement

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.

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.

Copyright Statement

Copyright (C) The Internet Society (2006). 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.

Acknowledgment

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