Network Working Group
Request for Comments: 5410
Obsoletes: 4909
Category: Informational

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

January 2009

Multimedia Internet KEYing (MIKEY) General Extension Payload for Open Mobile Alliance BCAST 1.0

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This document specifies a new Multimedia Internet KEYing (MIKEY) General Extension payload to transport the short-term key message (STKM) and long-term key message (LTKM) payloads as well as the management data LTKM reporting message and parental control message payloads defined in the Open Mobile Alliance's (OMA) Broadcast (BCAST) group's Service and Content protection specification.

Table of Contents

1. Introduction

The Multimedia Internet KEYing (MIKEY) protocol specification (RFC 3830 [RFC3830]) 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 [SPCP] specifies the use of a short-term key message (STKM), a long-term key message (LTKM), an LTKM reporting message, and 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 [RFC3830].

RFC 3830 [RFC3830], the MIKEY General Extension payload defined in RFC 4563 [RFC4563], and the 3rd Generation Partnership Project (3GPP)'s Multimedia Broadcast/ Multicast Service (MBMS) document [3GPP.33.246] specify the transport of MIKEY messages via unicast or broadcast; the OMA BCAST 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 [RFC2119].

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

The OMA BCAST Type (Type 5) formats the MIKEY General Extension payload as follows:

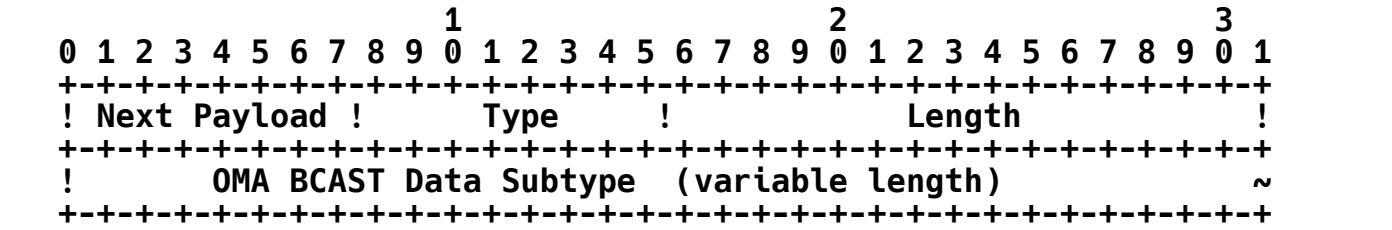

Figure 1: OMA BCAST MIKEY General Extension

Next Payload and Length are defined in Section 6.15 of [RFC3830].

Type (8 bits): identifies the type of the General Extension Payload (see Section 6.15 of [RFC3830]). This document adds a new type. It 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 OMA BCAST MIKEY General Extension Payload

OMA BCAST Data Subtype (variable length): defines a variable length Data field. This field is formed by subtype-payloads. The contents of the variable length OMA BCAST Data Subtype field are defined below.

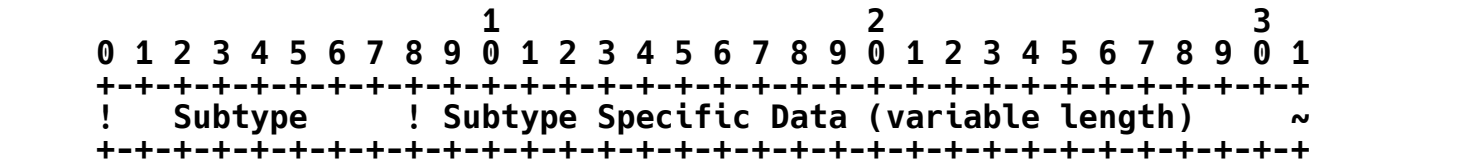

Figure 3: STKM/LTKM/LTKM Reporting/Parental Control Subtype Payload

Subtype: 8 bits. This field indicates the subtype of the OMA BCAST payload. In this specification, four values are specified: LTKM (1), STKM (2), LTKM Reporting (3), and Parental Control (4).

Subtype Specific Data: Variable length.

OMA BCAST Data Subtype	Value	Comment
LTKM	1	Long Term Key Message
STKM	2	Short Term Key Message
LTKM Reporting	3	LTKM Reporting Message
Parental Control	4	Parental Control Message

Figure 4: Subtype Definitions for OMA BCAST Messages

The contents of the OMA BCAST Data Subtype payload field are defined in Section 6 of the OMA BCAST Service and Content Protection specification [SPCP].

4. Interoperability Considerations

This document specifies the use of MIKEY General Extension payload Type 5 and four subtype values: 1 and 2 for OMA BCAST Service and Content protection's LTKM and STKM payloads (respectively), 3 for LTKM Reporting payload, and 4 for Parental Control payload. 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 [RFC3830] and RFC 4563 [RFC4563].

5. Security Considerations

According to RFC 3830 [RFC3830], 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 also covers 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" for use by OMA BCAST as requested by RFC 4909 [RFC4909]. Furthermore, IANA has created a name space for the OMA BCAST payload subtype values defined in [RFC4909] and has assigned the following subtype values from this name space: LTKM (1), STKM (2).

IANA has allocated two new subtypes from the OMA BCAST payload subtype name space.

The subtypes are as follows:

Subtype Name: LTKM Reporting

Value: 3

and

Subtype Name: Parental Control

Value: 4

7. Changes since RFC 4909

OMA BCAST Service and Content Protection specification [SPCP] 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 [RFC4909].

8. Acknowledgments

Many thanks to the authors of RFC 4909 [RFC4909] for allowing us to obsolete their RFC.

9. References

9.1. Normative References

[3GPP.33.246] 3GPP, "3G Security; Security of Multimedia Broadcast/ Multicast Service (MBMS)", 3GPP TS 33.246 6.12.0, October 2007.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3830] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, August 2004.

[RFC4563] 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.

[SPCP] Open Mobile Alliance, "Service and Content Protection for Mobile Broadcast Services", OMA-TS-BCAST_SvcCntProtection-V1_0, <http://www.openmobilealliance.org>.

9.2. Informative References

[RFC4909] Dondeti, L., Castleford, D., and F. Hartung, "Multimedia Internet KEYing (MIKEY) General Extension Payload for Open Mobile Alliance BCAST LTKM/STKM Transport", RFC 4909, June 2007.

Authors' Addresses

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

Phone: +49 89 636-45868
EMail: 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