Internet Engineering Task Force (IETF)
Request for Comments: 6309
Obsoletes: 4909
Updates: 3830, 4563, 5410, 6043
Category: Standards Track
ISSN: 2070-1721

J. Arkko
A. Keranen
J. Mattsson
Ericsson

August 2011

IANA Rules for MIKEY (Multimedia Internet KEYing)

Abstract

This document clarifies and relaxes the IANA rules for Multimedia Internet KEYing (MIKEY). This document updates RFCs 3830, 4563, 5410, and 6043; it obsoletes RFC 4909.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6309.

1. Introduction

This document relaxes the IANA rules for Multimedia Internet KEYing (MIKEY) [RFC3830]. The IANA rules defined in [RFC3830], [RFC4563], [RFC4909], and [RFC5410] are affected. In addition, the rules specified in [RFC6043] are re-specified here.

Most of the values in MIKEY namespaces are divided into two ranges: "IETF Review" (or "IETF Consensus" as it was previously called) and "Reserved for Private Use" [RFC5226]. This document changes, for majority of the namespaces, the requirement of "IETF Review" to "IETF Review or IESG Approval" [RFC5226]. For some namespaces, the requirement is changed to "Specification Required" [RFC5226].

The rationale for this update is that there can be situations where it makes sense to grant an allocation under special circumstances or that time has shown that the current requirement is unnecessarily strict for some of the namespaces. By changing the current IANA rules to also allow for "IESG Approval" [RFC5226], it becomes possible for the Internet Engineering Steering Group (IESG) to consider an allocation request, even if it does not fulfill the default rule. For instance, an experimental protocol extension could perhaps deserve a new payload type as long as a sufficient number of types still remains, and the MIKEY community is happy with such an allocation. Moreover, for some registries, a stable specification would be a sufficient requirement, and this is thus reflected in the updated IANA rules. For instance, an RFC via the Independent Stream at the RFC Editor is sufficient for some registries and does not force an IETF evaluation of a particular new extension for which there is no general demand. Nevertheless, "IETF Review" is still encouraged (instead of using the "IESG Approval" path) if there is doubt about whether or not it is needed for a new allocation.

The rest of this document is structured as follows. Section 2 defines the new IANA rules. Section 3 discusses the security implications of this document. Sections 4, 5, 6, and 7 explain the changes to [RFC3830], [RFC4563], [RFC4909], [RFC5410], and [RFC6043].

2. IANA Considerations

IANA updated the registries related to MIKEY as specified below. All other MIKEY IANA registries remain unchanged.

New values for the version field ([RFC3830], Section 6.1) and the C envelope key cache indicator ([RFC3830], Section 6.3) field can be allocated via "IETF Review".

The "IETF Review" requirement for adding new values into namespaces, originally defined in [RFC3830], is to be changed to "IETF Review or IESG Approval". This change affects the following namespaces:

- data type ([RFC3830], Section 6.1)
- Next payload ([RFC3830], Section 6.1)
- PRF func ([RFC3830], Section 6.1)
- CS ID map type ([RFC3830], Section 6.1)
- Encr alg ([RFC3830], Section 6.2)
- MAC alg ([RFC3830], Section 6.2)
- DH-Group ([RFC3830], Section 6.4)
- S type ([RFC3830], Section 6.5)
- TS type ([RFC3830], Section 6.6)
- ID Type ([RFC3830], Section 6.7)
- Cert Type ([RFC3830], Section 6.7)
- Hash func ([RFC3830], Section 6.8)
- SRTP Type ([RFC3830], Section 6.10)
- SRTP encr alg ([RFC3830], Section 6.10)
- SRTP auth alg ([RFC3830], Section 6.10)
- SRTP PRF ([RFC3830], Section 6.10)
- FEC order ([RFC3830], Section 6.10)
- Key Data Type ([RFC3830], Section 6.13)
- KV Type ([RFC3830], Section 6.13)

The "IETF Review" requirement for the following registries, originally defined in [RFC3830], [RFC4563], [RFC4909], and [RFC5410], is to be changed to "Specification Required".

- Prot type ([RFC3830], Section 6.10)
- Error no ([RFC3830], Section 6.12)
- General Extension Type ([RFC3830], Section 6.15)
- KEY ID Type ([RFC4563], Section 4)
- OMA BCAST Data Subtype ([RFC5410], Section 3)

The "Specification Required" requirement remains for the following namespaces:

- TS Role ([RFC6043], Section 6.4)
- ID Role ([RFC6043], Section 6.6)
- RAND Role ([RFC6043], Section 6.8)
- Ticket Type ([RFC6043], Section 6.10)

The range of valid values for certain namespaces defined in the IANA considerations of [RFC3830] was not explicitly defined and is clarified here as follows:

Namespace	Valid values
C Envelope Key Cache Indicator	0 - 3
S type	0 - 15
Key Data Type	0 - 15
KV Type	0 - 15

3. Security Considerations

This specification does not change the security properties of MIKEY. However, when new values are introduced without IETF consensus, care needs to be taken to assure that possible security concerns regarding the new values are still addressed.

4. Changes from RFC 3830

Section 2 relaxes the requirements from those defined in [RFC3830]. A number of namespaces now have the "IETF Review or IESG Approval" requirement, when they previously had the "IETF Review" requirement. In addition, some namespaces now have the "Specification Required" requirement.

5. Changes from RFC 4563

Section 2 relaxes the requirements from those defined in [RFC4563]. The KEY ID Type namespace now has the "Specification Required" requirement.

6. Changes from RFC 4909 and RFC 5410

Section 2 relaxes the requirements from those defined in [RFC4909]. The OMA BCAST Data Subtype namespace now has the "Specification Required" requirement. Note that [RFC5410] obsoleted [RFC4909] but does not actually define the IANA rules itself. As a result, from now on, this RFC defines the IANA requirements for the OMA BCAST Data Subtype namespace.

7. Changes from RFC 6043

There are no changes to the rules specified in [RFC6043]. However, for sake of completeness, Section 2 re-specifies these rules in this document, and from now on, this RFC defines the IANA requirements for those namespaces.

8. References

8.1. Normative References

[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.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5410] Jerichow, A. and L. Piron, "Multimedia Internet KEYing (MIKEY) General Extension Payload for Open Mobile Alliance BCAST 1.0", RFC 5410, January 2009.

[RFC6043] Mattsson, J. and T. Tian, "MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)", RFC 6043, March 2011.

8.2. 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

Jari Arkko
Ericsson
Jorvas 02420
Finland

EMail: jari.arkko@piuha.net

Ari Keranen
Ericsson
Jorvas 02420
Finland

EMail: ari.keranen@ericsson.com

John Mattsson
Ericsson
Stockholm SE-164 80
Sweden

EMail: john.mattsson@ericsson.com