Network Working Group	J. Arkko
Internet-Draft	A. Keranen
Updates: 3830, 4563, 5410, 6043 (if approved)	J. Mattson
Obsoletes: 4909 (if approved)	Ericsson
Intended status: Standards Track	May 20, 2011
Expires: November 21, 2011	

IANA Rules for MIKEY (Multimedia Internet KEYing) draft-arkko-mikey-iana-01

Abstract

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

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet- Drafts is at http://datatracker.ietf.org/drafts/current/.
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."
This Internet-Draft will expire on November 21, 2011.

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" into "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 allow also 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 hence this is reflected in the updated IANA rules. For instance, for some registries an RFC via the Independent Stream at the RFC Editor is sufficient, and does not force an IETF evaluation of a particular new extension for which there is no general demand.
This document also makes some small corrections to the existing IANA registries. (RFC Editor: Please remove this paragraph upon publication as an RFC.)
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. Section 4, Section 5, Section 6, and Section 7, explain the changes to the RFCs 3830, 4563, 4909, 5410, and 6043.

2. IANA Considerations

IANA is requested to update the registries related to MIKEY as specified below. All other MIKEY IANA registries are to remain unchanged.
A registry for the version field should be created, with the value 0x01 as the only currently allocated item. (RFC Editor: Please remove the preceding sentence upon publication as an RFC.) 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 requirement for adding new values into name spaces, originally defined in [RFC3830], and having requirement of "IETF Review" is to be changed into "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 into "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 Types ([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 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

(RFC Editor: please remove this paragraph before publication and when the IANA registry has been updated with the following changes) The current MIKEY IANA registry defines sub-registries with explicit name for certain parameters (e.g., Next Payload) whereas other parameters (e.g., Encr alg) have no (explicit) sub-registries. IANA is requested to define explicit sub-registries for all the parameters with sub-registry names matching the names used in this document.

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 Types 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 Type 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 Arkko Ericsson Jorvas, 02420 Finland EMail: jari.arkko@piuha.net

Ari Keranen Keranen Ericsson Jorvas, 02420 Finland EMail: ari.keranen@ericsson.com

John Mattson Mattson Ericsson Stockholm, SE-164 80 Sweden EMail: john.mattsson@ericsson.com

Table of Contents