Networking Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 13, 2012

R. Alexander
T. Tsao
Cooper Power Systems

July 12, 2011

Adapted Multimedia Internet KEYing (AMIKEY): An extension of Multimedia Internet KEYing (MIKEY) Methods for Generic LLN Environments draft-alexander-roll-mikey-lln-key-mgmt-01

Abstract

Multimedia Internet Keying (MIKEY) is a key management protocol used for real-time applications. As standardized within RFC3830 it defines four key distribution methods, including pre-shared keys, public-key encryption, and Diffie-Hellman key exchange, with allowances for ready protocol extension. A number of additional methods have been developed and continue to be built from the base protocol (see for example, RFC4442, RFC4563, RFC4650, RFC4738, RFC5410, RFC6043 and RFC6267. However, in spite of its extensibility and more general applicability, MIKEY and its related extensions have primarily focused on the support of the Secure Real-time Transport Protocol (SRTP).

This document specifies a simple adaptation of the MIKEY specification to allow the base protocol and its various key management mode extensions to be readily applied in more general environments beyond the multimedia SRTP domain. In particular, the document defines a repurposing of the MIKEY multimedia crypto sessions structure and introduces a set of message extensions to the base specification to allow the MIKEY key management methods to be applied within Low-power and Lossy networks (LLNs) and other general constrained-device networks.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

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 January 13, 2012.

Copyright Notice

Table of Contents

1. Introduction

Any sufficiently large scale network offering security services requires an automated key management mechanism for the exchange of keys and the update of related security credentials [RFC4107]. Key management may be needed for individual session exchanges or for the long-term control and update of security parameters from which session keys may be derived. In many Low-power and Lossy networks (LLN) and other constrained-device environments, key management emphasis is often on the management of long-term keys. This may automatically follow network associations based on device pre-configuration or may be based on specified key lifetimes or administrative or event-driven need for key credential changes. This would apply to the case of a network routing protocol like RPL ([I-D.ietf-roll-rpl]) that employs security as well as to other secured communications layer protocols.

Multimedia Internet Keying (MIKEY) is a key management protocol that has been used for real-time applications both for peer-to-peer and group communications. The capabilities of the protocol lend themselves just as readily to the management of long-term keys as to per-session or per association key control. MIKEY [RFC3830] defines four key distribution methods including pre-shared keys, public-key encryption, and Diffie-Hellman key exchange. Given its design simplicity, efficiency and flexibility a number of additional modes and extensions have indeed been developed and continue to be built from the base protocol (see for example, [RFC4442], [RFC4563], [RFC4650], [RFC4738], [RFC5410], [RFC6043] and [RFC6267]). MIKEY and its related RFC extensions have however primarily focused on the support of the SRTP and related Session Initiation Protocol (SIP) call scenarios [RFC3711].

This document specifies an adaptation of the MIKEY protocol specification to allow the base protocol and its various key management mode extensions to be more generally applied to LLN environments. In particular, the document defines a repurposing of the MIKEY multimedia crypto sessions structure to allow optional support for simultaneous management of multiple protocol or device interface key. The specification also introduces a set of message extensions to the base MIKEY protocol to allow its key management methods to be applied within generic LLN and constrained-device networks.

1.1. Motivation

Key distribution describes the process of delivering cryptographic keys to the required communicating parties. The MIKEY protocol has defined the mechanisms for establishing the security context used by

SRTP however the mechanisms for security parameter negotiation and update is just as readily extended to LLN protocols.

The flexibly to employ different key distribution methods according to available network infrastructure and particular operating scenarios together with the compact efficiency of its binary specification makes MIKEY well suited for general LLN use. The wide range of key management support extending from light-weight, low latency half round-trip pre-shared key distribution methods to multi-exchange Diffie-Hellman key agreements protected with digital signatures or pre-shared keys offers great flexibility to meet the needs of diverse LLN application environments.

The option to embed the MIKEY key management messages within an existing network signaling protocol or to be directly transported or UDP or TCP (using port 2269) also increases the ability to apply the methods in more general LLN domains.

MIKEY has met its original stated design goals [RFC3830] of end-to-end security, simplicity, efficiency, tunneling (even beyond integration with Session Description Protocol (SDP) [RFC4566] or RTCP [RFC3605]), and independence of underlying transport. In so doing it offers an excellent base for a generic key management protocol for Low-power Lossy Network (LLN) application. Key management protocols are also difficult to design and validate (see [RFC4107] guidelines) providing a further motivation for reliance on an established protocol like MIKEY that has had the benefit of wider operational deployment and evaluation.

1.2. MIKEY Key Management Methods Background

As noted in [RFC5197], several key distribution methods have been described for MIKEY, including:

- Symmetric key distribution as defined in [RFC3830] (MIKEY-PSK)
- Asymmetric key distribution as defined in [RFC3830] (MIKEY-RSA)
- Diffie-Hellman key agreement protected by digital signatures as defined in [RFC3830] (MIKEY-DHSIGN)
- Diffie-Hellman key agreement protected by symmetric pre-shared keys as defined in [RFC4650] (MIKEY-DHHMAC)
- Asymmetric key distribution (based on asymmetric encryption) with in-band certificate provision as defined in [RFC4738] (MIKEY-RSA-R)

Further extensions to MIKEY comprising algorithm enhancements and new payload definitions have since been defined generally motivated by the specific problems associated with SIP signaling and associated multimedia use case scenarios (see [RFC5197]for an earlier assessment). This specification proposes a new extension that is focused on a new domain of application.

1.3. Adapting MIKEY to General LLNs

This document specifies is a set of additional message information elements to the base MIKEY protocol that provide both algorithm and message payload extensions. These additions allow the adapted protocol to be used directly for key transport and security policy specification between communications generic network entities. Furthermore, through integration within the base MIKEY specification it will allow current and future key methods and extensions to be utilized outside of the current multimedia environment.

The developed protocol adaption includes the specification of alternative default algorithms (in particular AES-based) and configurations that are particular to more constrained communications devices and using MIKEY’s general extensibility to define new elements applicable to the LLN environment.

An important element of the protocol extension is the re-use of the MIKEY crypto-session structure to apply to individual device communications protocol layers or interfaces instead of applying to multimedia streams. By maintaining this base protocol structure and re-purposing associated message identifiers, the specification minimizes the protocol changes needed for network adaptation.

As with the original specification the intent is to allow MIKEY messages to be embedded into existing communications signaling protocols or to be independently transported between communicating entities over UDP or TCP transport connections.

Note: While MIKEY and its extensions provide a variety of choices in terms of modes of operation, implementations for a given LLN application domain will be able to simplify node behavior by operating in a single mode. To ensure necessary interoperability within the LLN environment, mandatory methods within the Adapted MIKEY protocol (AMIKEY), akin to those of MIKEY, shall be specified.

1.4. Terminology and Definitions

The following definitions have been taken from [RFC3830] with necessary augmentation for AMIKEY as indicated:

(Data) Security Protocol
: The security protocol used to protect the actual data traffic. Examples of security protocols are IPsec and SRTP. For generic LLNs, security protocols may include secure versions of protocols such as RPL [I-D.ietf-roll-rpl].

Data SA
: Data Security Association information for the security protocol, including a TEK and a set of parameters/policies.

CS
: Crypto Session, uni- or bidirectional data stream(s) protected by a single instance of a security protocol. For AMIKEY the concept of a crypto-session is expanded to allow definition of a particular protocol layer, logical device interface, or other communications association for which key management support is provided.

CSB
: Crypto Session Bundle, collection of one or more Crypto Sessions, which can have common TGKs (see below) and security parameters.

CS ID
: Crypto Session ID, unique identifier for the CS within a CSB. For AMIKEY the CS ID is used to identify a specific protocol layer, logical device interface or other communications association for which AMIKEY is being used to support key management (establishment of re-keying update).

CSB ID
: Crypto Session Bundle ID, unique identifier for the CSB. For AMIKEY the CSB ID in conjunction with the Timestamp filed is used as a unique key management exchange message reference identifier. This identifier will allow for the acknowledged key management message exchanges where applicable. The ID plus timestamp will also support the filtering of repeated or redundant AMIKEY messages when key management occurs over an unreliable transport network.

TGK
: TEK Generation Key, a bit-string agreed upon by two or more parties, associated with CSB. From the TGK, Traffic-Encrypting Keys can then be generated without needing further communication.

TEK
: Traffic-Encrypting Key, the key used by the security protocol to protect the CS (this key may be used directly by the security protocol or may be used to derive further keys depending on the security protocol). The TEKs are derived from the CSB's TGK.

The following definitions have been added to the ones from [RFC3830] specifically related to supporting AMIKEY:

Key Index
: The Key Index (KI) is used as identifier to allow for reference to the key(s) that are associated with a given CS. Where TEKs may be updated over time a TGK can be associated with a KI that is transported as a payload within the AMIKEY message from the Initiator. Any TEK generated from the AMIKEY TGK shall be assigned the key index value associated with the TGK. Within general LLN protocol communications related to a given CS (device layer protocol or interface), to ensure security association synchronization reference can be made to the key index that is being applied for the given protocol security. Following successfully TGK key establishment communicating devices can verify security contexts through reference to maintained KI (see Section 6.16).

Key Source Identifier
: The Key Source Identifier (KSI) is used as a logical identifier to allow for refernece to the entity associated with the origination of a given TGK. Where TEKs are dynamically generated or updated, each TGK can be associated with a specific key source. The KSI, when used, is transported as a payload within the AMIKEY message from the entity responsible for the TGK origination (see Section 6.17).

1.5. Document Outline

Section 2 provides a brief general system overview of key management as introduced in MIKEY specification. This section generalizes the context in which the Adapted MIKEY (AMIKEY) protocol extension is applied. It also provides a reference to the common key management operating base of MIKEY and AMIKEY.

Sections 3 to 4 go into further detail by identifying the specific section and subsection extensions and enhancements needed to support the MIKEY protocol adaptation. These Sections mirror those of MIKEY [RFC3830] and are used to show the necessary commonality and make reference to specific changes would be required for AMIKEY. Reference is made only to the applicable Sections and Subsections of [RFC3830] for which special changes are proposed.

Section 6 includes the specific protocol specification elements that are needed to extend MIKEY for the support of the generic LLN key management requirements.

The remaining document sections are place-holders for standard RFC

draft sections.

1.6. Section Headings Notation

This document is written as a delta document to [RFC3830]. For ease of cross-reference and to maintain consistency with the MIKEY specification document structure, Section heading and Table and Figure numbers are maintained consistent with the [RFC3830] usage.

The notation of Section number followed by [RFC3830] "x.x. [RFC3830]" is used is this document for Sections specifically meant to align with [RFC3830]. Section numbers followed by [RFC3830] with additional heading text indicates some new element or clarification introduced by this specification. Section numbers followed by [RFC3830] without further heading text implies no change to [RFC3830] and is used only to align and maintain the current document headings structure.

The new parameters introduced in this specification are made consistent with the MIKEY recommendations (see Section 4.2.9 [RFC3830]).

2. AMIKEY Overview

This section provides an overview of AMIKEY. Material from MIKEY [RFC3830] is also repeated to clearly establish the common context in which MIKEY can be applied to LLN environments with the simple extension to the Adapted MIKEY (AMIKEY) specification.

The objective of the AMIKEY extension is exactly the same as that of MIKEY - "to produce a data security association (SA) for a security protocol, including a Traffic-Encrypting Key (TEK), which is derived from a TEK Generation Key (TGK), and used as input for the security protocol." In the case of AMIKEY the objective is support generic security protocols and particularly those that may be associated with LLNs.

AMIKEY uses the specified MIKEY mechanisms and features to "support the possibility of establishing keys and parameters for more than one security protocol (or for several instances of the same security protocol) at the same time." In MIKEY the Crypto Session Bundle (CSB), which derives from the multimedia (multi-stream) context, is used to denote this collection of one or more Crypto Sessions that can have a common TGK and security parameters, but that obtain distinct TEKs from MIKEY.

In the AMIKEY extension, the concept of CSB is used to provide the

option of simultaneously establishing multiple SAs on a given device. The individual Crypto Session (CS) SAs may be associated with different device layer or device interface security protocols. AMIKEY further uses the flexibility of the MIKEY specification to allow separate security policies to be defined in the SA established for each security protocol. The distribution mechanisms defined by MIKEY for re-keying and updating of established security associations is hence also directly applied. The ability to establish and maintain multiple SAs through a single key management association provides an important efficiency element in LLN domains.

As specified in [RFC3830], Section 2.3, the procedure of setting up a CSB and creating a TEK (and Data SA), is done in accordance with Figure 1:

1. A set of security parameters and TGK(s) are agreed upon for the Crypto Session Bundle. This is done by one of many alternative key transport/exchange mechanisms (see [RFC3830], Section 3, as well as subsequent extension RFCs).

2. The TGK(s) is used to derive (in a cryptographically secure way) a TEK for each Crypto Session or associated security protocol.

3. The TEK, together with the security protocol parameters, represent the Data SA, which is used as the input to the security protocol(s).

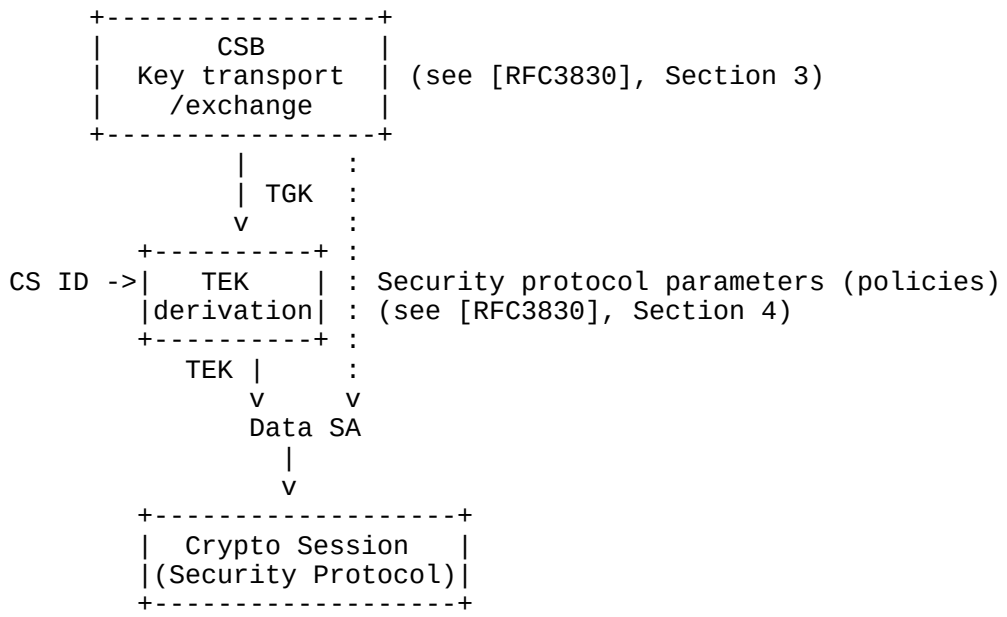


Figure 1: Overview of MIKEY (and AMIKEY extension) key management procedure

For generic LLNs that are the focus of this document, the default algorithms applied in the generation of the TEK for each protocol is defined within this AMIKEY specification. An additional MIKEY message extension is also specified to define the security protocol parameters (policies) for generic LLNs.

Whereas MIKEY CS IDs are associated with multimedia streams and have no intrinsic designation, in this specification the CS IDs are assigned values (public or private/vendor-specific) that are used to identify security protocols associated with specific device protocol layers or device interfaces.

As considered for the device security model discussed in [I-D.ietf-roll-security-framework], Section 6.5, Figure 2 provides an overview of the key management context introduced by the AMIKEY extension defined in this specification. The multi-protocol key management capability (through the particular use of the MIKEY CS-IDs) allows for the efficient, simultaneous management and update of one or more protocol layer security parameters.

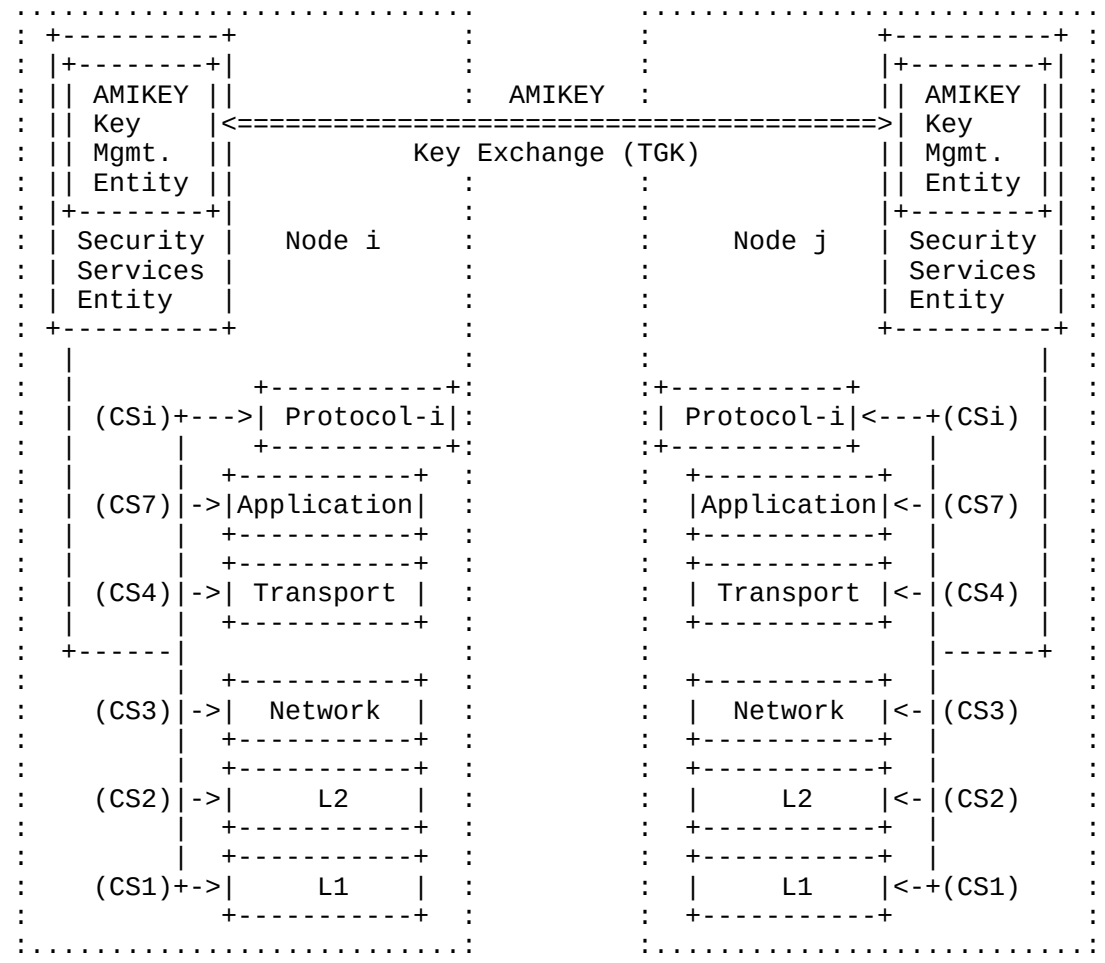


Figure 2: Overview of AMIKEY Multi-protocol Key Management Context

As in the base MIKEY specification, the security protocol can either use the TEK directly, or, if supported, derive further session keys from the TEK. It is however up to the targeted security protocol and the associated security policy to define how the TEK is used.

MIKEY can be used to update TEKs and the Crypto Sessions in a current Crypto Session Bundle (see [RFC3830], Section 4.5). This is done by executing the transport/exchange phase once again to obtain a new TGK (and consequently derive new TEKs) or to update some other specific CS parameters.

3. AMIKEY Extension Elements

The following Section and Subsections detail the proposed additions to the MIKEY specification [RFC3830] to support the AMIKEY extension. The Section heading outline of the MIKEY specification is used to indicate the delta changes made by the AMIKEY extension.

3.1. [RFC3830] Pre-shared key

3.2. [RFC3830] Public-Key Encryption

3.3. [RFC3830] Diffie-Hellman Key Exchange

4. [RFC3830] Selected Key Management Functions

For AMIKEY all the key derivation functionality defined in MIKEY shall be based on a new default Pseudo-Random Function (PRF) given by the AES-based, AES-XCBC-PRF-128 algorithm as specified in [RFC4434].

4.1. [RFC3830] Key Calculation

4.1.1. [RFC3830] Assumptions

For AMIKEY cs_id is defined so that session represents a protocol layer, logical device interface, or communications association. The cs-id values shall be as defined in this specification (see Section 6.1.2) and may be public or private/vendor-specific.

4.1.2. [RFC3830] Default PRF Description

For AMIKEY the default pseudo random function shall be AES-XCBC-PRF-128 [RFC4434]. Note: AES-XCBC-PRF-128 aligns with HMAC-SHA1 and HMAC-MD5 as PRFs.

4.1.3. [RFC3830] Generating Keys from TGK

For AMIKEY the cs-id values shall be as defined in this specification (see Section 6.1.2).

4.1.4. [RFC3830] Generating Keys for MIKEY Messages from an Envelope/ Pre-shared Key

Change from default PRF to the default AMIKEY PRF given in Section 4.1.2 of this specification.

Note: For AMIKEY, the Authentication key constant SHALL be used for generating the single TEK in the case of authenticated encryption

algorithms (such as AES-CCM).

4.2. [RFC3830] Pre-defined Transforms and Timestamp Formats

4.2.1. [RFC3830] Hash Functions

For AMIKEY the default hash function shall be AES-XCBC-PRF-128 [RFC4434].

4.2.2. [RFC3830] Pseudo-Random Number Generator

For AMIKEY it shall be MANDATORY to implement the new default AES-XCBC-PRF-128 PRF specified in [RFC4434] (See Section 4.1.2 of this specification).

4.2.3. [RFC3830] Key Data Transport Encryption

As in MIKEY the default and mandatory-to-implement key transport encryption shall be AES in Counter mode using a 128-bit key (derived as defined in Section 4.1.4 above). The applied Counter shall be the IV defined in [RFC3830], Section 4.2.3.

4.2.4. [RFC3830] MAC Verification Message Function

For AMIKEY AES-CCM-64 shall be the defined default for key message authentication. The Counter used shall be the IV defined in [RFC3830], Section 4.2.3.

4.3. [RFC3830] Certificates, Policies and Authorization

4.4. [RFC3830] Retrieving the Data SA

For AMIKEY the retrieval of a Data SA will depend on the security protocol. The support for different security protocols shall be explicitly identified through the use of public CS ID values (see Section 6.1.2 of this specification).

5. [RFC3830] Behavior and Message Handling

6. [RFC3830] Payload Encoding

The generic LLN security protocol parameters may be transported between peers as part of a key establishment or re-keying exchange. Based on IANA registration, MIKEY currently only defines two payloads for transporting the security policy information (see Section 6.10 of [RFC3830] and [RFC4442]). This section describes the extension of

MIKEY to allow the transport of Generic LLN security policy information and associated key(s) as well as applicable PRF used for key derivation.

This section describes, in detail, the payload for support of the Generic LLN security protocol(s) specified by the Adapted MIKEY protocol. As in RFC3830, for all encoding, network byte order is always used, and the sign ~ indicates a variable length field.

6.1. [RFC3830] Common Header Payload (HDR)

The Common Header payload MUST always be present as the first payload in each message. The Common Header includes a general description of the exchange message.

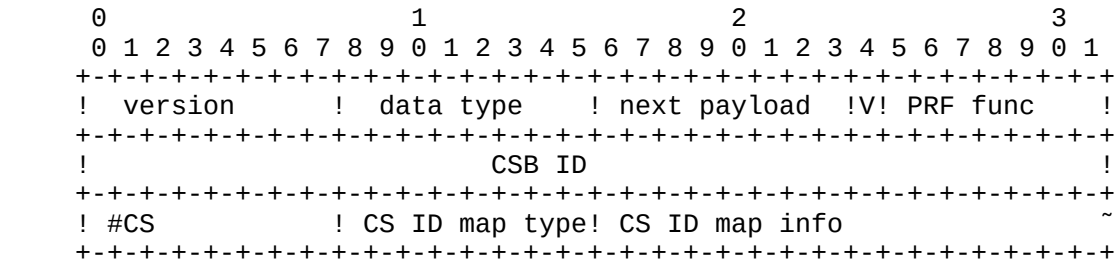


Figure 3: Common Header [RFC3830]

- version (8 bits): the version number of MIKEY.
- version = 0x01 refers to MIKEY as defined and maintained in [RFC3830].
- version = 0x03 (to be assigned by IANA) shall be used to refer to AMIKEY as defined and maintained in this document.
- data type (8 bits): describes the type of message (e.g., public-key transport message, verification message, error message). See latest IANA registered values. No additional values are specified for AMIKEY (TBD).
- next payload (8 bits): identifies the payload that is added after this payload. See latest IANA registered values.

For AMIKEY a new next payload value is assigned to carry the Key Index parameter (see also Section 6.16).

Next Payload	Value	Section
Last payload ...	0	-
Key Index	n	Section 6.16 as given by the AMIKEY specification (value to be assigned by IANA).
Key act time	m	Section 6.18 as given by the AMIKEY specification (value to be assigned by IANA)

Table 6.1.b

- V (1 bit): flag to indicate whether a verification message is expected or not (this only has meaning when it is set by the Initiator).

- PRF func (7 bits): indicates the PRF function that has been/will be used for key derivation; for AMIKEY a new value, 2, has been specified to indicate the PRF that must be supported for LLNs.

PRF Function	Value	Comments
AES-XCBC-PRF-128	2	As specified in [RFC4434] and that shall be mandatory for AMIKEY

Table 6.1.c

(AMIKEY value to be assigned by IANA)

- CSB ID (32 bits): identifies the CSB (generated as specified in [RFC3830]); for AMIKEY this field is used as a message reference identifier to allow for duplicate detection where message exchanges occur over an unreliable transport network.

- #CS (8 bits): indicates the number of Crypto Sessions that will be handled within the CBS; for AMIKEY this field indicates the number of protocol layers, logical device interfaces, or other communications associations that are being configured or managed within the current key management message exchange.

- CS ID map type (8 bits): specifies the method of uniquely mapping. Crypto Sessions to the security protocol sessions; for AMIKEY a new value, 3, has been specified to indicate the Generic-LLN map

type that must be supported for LLNs.

CS ID Map Type	Value	Comments
Generic_LLN-ID	3	As specified in this document and as mandatory for AMIKEY

Table 6.1.d

(AMIKEY value to be assigned by IANA)

- CS ID map info (variable length): identifies the crypto session(s) for which the SA should be created. For AMIKEY the GENERIC_LLN map type (defined in Section 6.1.2 below) is used to specify the security association for the individual protocol layers, logical device interfaces, or other communications associations for which key management is being provided.

6.1.1. [RFC3830] SRTP ID

6.1.2. The Generic_LLN-ID Map Type

For the Generic_LLN map type, the CS ID map info consists of #CS (see Section 6.1) number of blocks or segments, where each segment maps policies (and a key) to a specific protocol layer, logical device interface or other communications association security protocol.

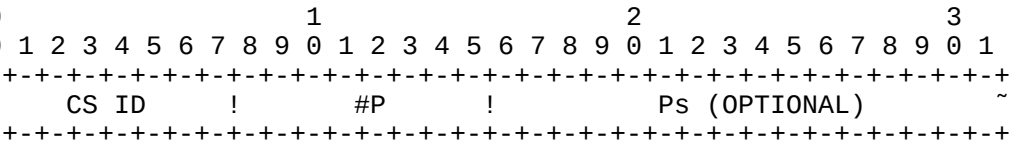


Figure 4: Generic_LLN-ID Map Type

- CS ID (8 bits): specifies the CS ID used to identify a given security protocol; for AMIKEY, when used in conjunction with the Generic-LLN map type, values 0-127 shall be reserved for assignment (by IANA) to specific protocol layer, logical device interface, or other communications association security protocols while values 128-255 shall be Reserved for Private Use.

Note: A combination of public and private CS IDs can be specified

within a given CSB when combined key management is being applied.

The following values are currently specified in this document (for example, with values to be assigned by IANA):

CS ID	Value	Comments
Reserved	0	
Generic PHY Layer	1	
Generic Link Layer	2	
Generic Network Layer	3	
Generic Transport Layer	4	
Generic Application Layer	7	
RPL Protocol	20	
...		
Reserved values	128-255	Reserved for private use

Table 6.1.e

- #P (8 bits): indicates the number of security policies provided for the crypto session (given by the CS ID) for which key management is being provided. In response messages, #P SHALL always be exactly 1. So if #P = 0 in an initial message, a security profile MUST be provided in the response message. If #P > 0, one of the suggested policies SHOULD be chosen in the response message. If needed, the suggested policies MAY be changed.

- Ps (variable length): lists the policies for the crypto session for which key management is being provided. It SHALL contain exactly #P policies, each having the specified Prot type (see Section 6.10.

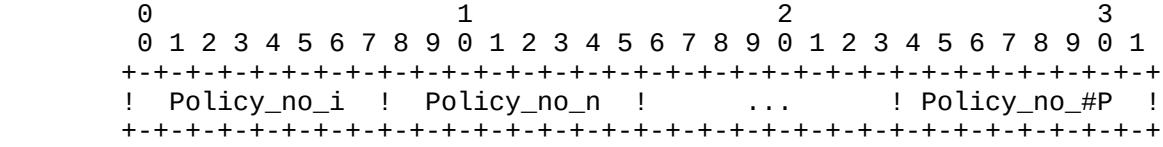


Figure 5: Policies

- Policy_no_i (8 bits): a policy_no that corresponds to the policy_no of a SP payload. In response messages, the policy_no may refer to a SP payload in the initial message. The policy numbers should be listed in increasing order.

6.2. [RFC3830] Key Data Transport Payload (KEMAC)

This section shall apply entirely as specified for MIKEY in [RFC3830] with the addition of the specific message authentication code algorithms given below for AMIKEY.

- MAC alg (8 bits): specifies the authentication algorithm used.

MAC alg	Value	Comments	Length (bits)
NULL	0	restricted usage [RFC3830], Section 4.2.4	0
HMAC-SHA-1-160	1	Mandatory, [RFC3830], Section 4.2.4	160
HMAC-SHA-256-256	2	Mandatory, [RFC3830], Section 4.2.4	256
AES-CBC-MAC-32	3	Mandatory for AMIKEY, see Section 4.2.4	32
AES-CBC-MAC-64	4	Mandatory for AMIKEY, see Section 4.2.4	64
AES-CBC-MAC-128	5	Mandatory for AMIKEY, see Section 4.2.4	128

Table 6.2.b

(Values for AMIKEY to be assigned by IANA)

- MAC (variable length): the message authentication code of the entire message.

For AMIKEY the use of AES-CBC-MAC-n may be applied in conjunction with the AES-CM encryption as given by the Encr alg field. This authenticated encryption shall be applied using an AES-CCM-n implementation.

6.3. [RFC3830] Envelope Data Payload (PKE)

6.4. [RFC3830] DH Data Payload (DH)

6.5. [RFC3830] Signature Payload (SIGN)

6.6. [RFC3830] Timestamp Payload (T)

6.7. [RFC3830] ID Payload (ID)

For AMIKEY the range of ID types shall be extended to allow for an expanded array of communications protocol entities that may be key management participants. The IDs are carried within the key management message ID payload field with the TLV format as specified in [RFC3830], Section 6.7.

ID Type	Value	Comments
IPv6 Address	4	As specified for AMIKEY
Device MAC Address	5	As specified for AMIKEY
Other (TBD)	n	As specified for AMIKEY

Table 6.7.a

The IPv6 Address ID type is used to allow an IPv6 Address to be referenced as the unique entity identifier of the key management correspondents. To directly reference the IPv6 Address of the exchanged packets, the ID len value will be set to zero and no ID data included in the value field.

The Device MAC Address is used to allow a MAC address to be referenced as the unique entity identifier for correspondents in a key management exchange.

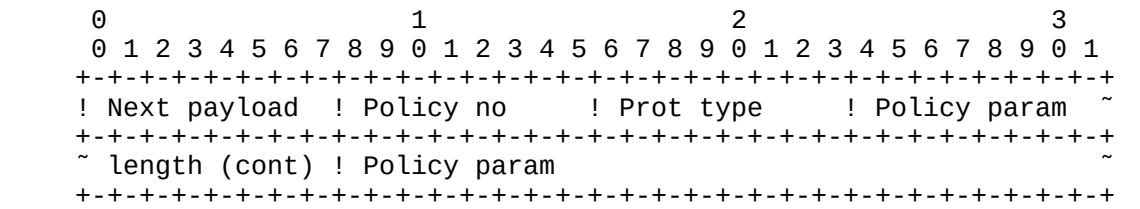
6.8. [RFC3830] Cert Hash Payload (CHASH)

6.9. [RFC3830] Ver msg payload (V)

6.10. [RFC3830] Security Policy (SP) Payload

The Security Policy payload defines a set of policies that apply to a specific security protocol.

For AMIKEY the definition is based on the same security policy payload definition in [RFC3830], Section 6.10, with a new security protocol (Generic-LLN) as defined below.



- Next payload (8 bits): Identifies the payload that is added after this payload. See Section 6.1 of [RFC3830] for more details.

- Policy no (8 bits): Each security policy payload must be given a distinct number for the current MIKEY session by the local peer. This number is used to map a cryptographic session to a specific policy (see also Section 6.1.1 of [RFC3830]).

- Prot type (8 bits): This value defines the security protocol; For AMIKEY an additional value shall be assigned as given below.

Prot Type	Value	Comments
Generic_LLN	3	As specified for AMIKEY

Table 6.10

- Policy param length (16 bits): This field defines the total length of the policy parameters for the selected security protocol.

- Policy param (variable length): This field defines the policy for the specific security protocol. The Policy param part is built up by a set of Type/Length/Value (TLV) payloads. For each security protocol, a set of possible type/value pairs can be negotiated as defined.

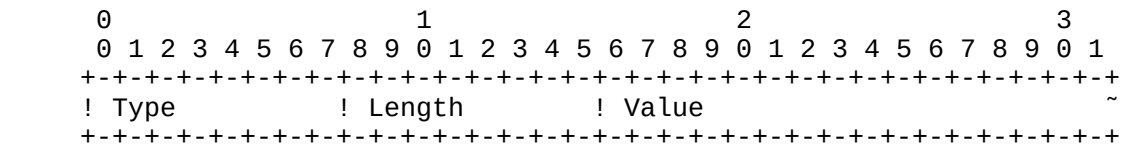


Figure 6: Policy Parameter

- Type (8 bits): Specifies the type of the parameter.
- Length (8 bits): Specifies the length of the Value field (in bytes).
- Value (variable length): Specifies the value of the parameter.

6.10.1. [RFC3830] SRTP Policy

6.10.2. AMIKEY Generic_LLN Policy

This policy specifies the parameters for the Generic_LLN (G_LLN) protocol for which key management is being provided. The types/values that can be negotiated are defined by the following table for the known, assigned CS ID values. For Vendor-specific, private CS ID values the applicable policy specification for a given crypto session will be left to the communicating parties.

Type	Meaning	Possible Values
0	Encryption algorithm	See below
1	Encryption key length	Depends on cipher used
2	Authentication algorithm	See below
3	Authentication key length	Depends on MAC used
4	Generic LLN PRF	See below
5	Encryption off/on	0 if off, 1 if on

Table 6.10.2.a

For the Encryption algorithm, a one byte length is sufficient. For AMIKEY the currently defined possible Values are:

G_LLN encr alg	Value
NULL	0
AES-CM-128	1

Table 6.10.2.b

For the Authentication algorithm, a one byte length is sufficient. For AMIKEY the currently defined possible Values are:

G_LLN auth alg	Value	Comments
NULL	0	Not recommended for operational use
AES-CBC-MAC-32	1	
AES-CBC-MAC-64	2	
AES-CBC-MAC-128	3	
RSA-SHA-256 Sig	4	

Table 6.10.2.c

Note: Since authentication is mandatory for operational protocol security, where Encryption is set "on" by the Generic_LLN policy, authenticated encryption, AES-CCM-n, with the MAC size given by the selected authentication algorithm, or AES-CM with authentication given by the identified Signature algorithm, shall be applied.

For the Generic_LLN pseudo-random function, a one byte length is also sufficient. For AMIKEY the currently defined possible Values are:

Generic_LLN PRF	Value
AES-XCBC-PRF-128	0

Table 6.10.2.d

6.11. [RFC3830] RAND Payload (RAND)

6.12. [RFC3830] Error Payload (ERR)

6.13. [RFC3830] Key Data Sub-Payload

6.14. [RFC3830] Key Validity Data

6.15. [RFC3830] General Extension Payload

6.16. Key Index Payload

For AMIKEY the Key Index (KI) payload is used to specify the value of the key index associated with a given TGK.

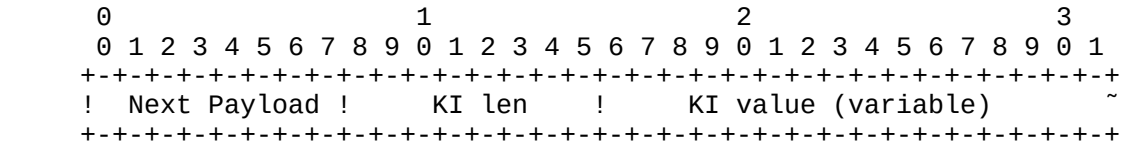


Figure 7: Key Index

- Next payload (8 bits): identifies the payload that is added after this payload. See Section 6.1 [RFC3830] for values.
- KI len (8 bits): indicates the length of the key source identifier field.
- KI value (variable length): indicates the value of the key index to be assigned to any CS TEK generated from the transported TGK.

6.17. Key Source Identifier Payload

For AMIKEY the Key Source Identifier payload is used to provide a logical reference to the entity associated with the origination of a given TGK. The specification of the Key Source Identifier (KSI) shall be given by the supported security protocol (for example, the secured RPL routing protocol [I-D.ietf-roll-rpl] specifies the use of an 8-byte KSI).

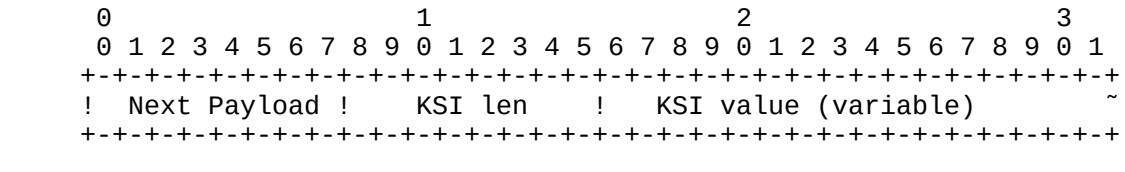


Figure 8: Key Source Identifier

- o Next payload (8 bits): identifies the payload that is added after this payload. See Section 6.1 [RFC3830] for values.
- o KSI len (8 bits): indicates the length of the key source identifier field.
- o KSI value (variable length): specifies the logical identifier assigned to the Source or Originator of a given TGK.

6.18. Key Activation Time Payload

For AMIKEY the Key Activation time payload is used to specify the time at which a new key derived from a communicated TGK shall become active for the associated device protocol or interface. The Key Activation time is used only when needed to specify a delay or future activation of an updated key. The format of this AMIKEY information element type shall be the same as that of the Timestamp payload (T) [RFC3830].

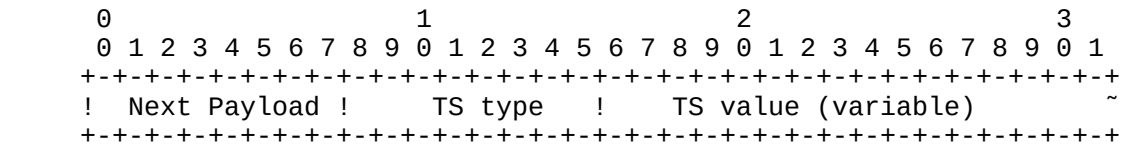


Figure 9: Key Activation Time Payload

- o Next payload (8 bits): identifies the payload that is added after this payload. See Section 6.1 [RFC3830] for values.
- o TS type (8 bits): indicates the timestamp type use to convey the time at which a new derived TEK shall become active (See Section 6.6 [RFC3830]).

- o TS value (variable length): the timestamp value of the specified TS type (See Section 6.6 [RFC3830]).

7. [RFC3830] Transport Protocols

As in [RFC3830], AMIKEY may be integrated within session establishment or other system signaling protocols or may be directly transported over UDP or TCP. Where AMIKEY messages are integrated into other LLN-related signaling protocols its transport shall be defined as part of those protocols.

8. Security Considerations

A primary motivation for this RFC is the security that comes from a re-use of the key management methods and framework developed for MIKEY. The extensive deployment and on-going development provides the benefit of much wider vetting and validation essential to assuring greater security.

9. [RFC3830] Groups

10. Additional Specification Considerations

Work had been previously initiated in developing support for an ECC-based asymmetric key management method ([I-D.ietf-msec-mikey-ecc], expired). In the context of LLNs application and subject to IPR considerations, related AMIKEY requirements may be developed.

11. IANA Considerations

This document defines several new name spaces associated with the AMIKEY payloads. This section summarizes the name spaces for which IANA is requested to manage the allocation of values. IANA is requested to record the pre-defined values defined in the given sections for each name space. IANA is also requested to manage the definition of additional values in the future. Unless explicitly stated otherwise, values in the range 0-240 for each name space SHOULD be approved by the process of IETF consensus and values in the range 241-255 are reserved for Private Use, according to [RFC2434].

The name spaces for the new fields identified in this document are requested to be managed by IANA (in bracket is the reference to the table with the initially registered values):

- Common Header payload (6.1.)
  - Version
- Next payload (6.1.b)
  - Key index
  - Key source identifier
  - Key activation time
- Prf func (6.1.c)
  - AES-XCBC-PRF-128
- CS ID map type (6.1.d)
  - Generic_LLN-ID
- MAC alg (6.2.b)
  - AES-CBC-MAC-32
  - AES-CBC-MAC-64
  - AES-CBC-MAC-128
- ID payload (6.7.a)
  - IPv6 Address
  - Device MAC Address
- Proto type (6.10)
  - Generic_LLN
- Generic_LLN policy (6.10.2)
  - Policy parameters (6.10.2.a)
  - G_LLN encr alg (6.10.2.b)
  - G_LLN auth alg (6.10.2.c)
  - G_LLN prf (6.10.2.d)

12. Acknowledgments

The authors would like to acknowledge the review and comments from Rene Struik.

13. References

13.1. Normative References

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

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

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

[RFC4434] Hoffman, P., "The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)", RFC 4434, February 2006.

13.2. Informative References

[I-D.ietf-msec-mikey-ecc] Milne, A., "ECC Algorithms for MIKEY", draft-ietf-msec-mikey-ecc-03 (work in progress), June 2007.

[I-D.ietf-roll-rpl] Winter, T., Thubert, P., Brandt, A., Clausen, T., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., and J. Vasseur, "RPL: IPv6 Routing Protocol for Low power and Lossy Networks", draft-ietf-roll-rpl-19 (work in progress), March 2011.

[I-D.ietf-roll-security-framework] Tsao, T., Alexander, R., Dohler, M., Daza, V., and A. Lozano, "A Security Framework for Routing over Low Power and Lossy Networks", draft-ietf-roll-security-framework-06 (work in progress), June 2011.

[RFC3605] Huitema, C., "Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)", RFC 3605, October 2003.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

[RFC4107] Bellovin, S. and R. Housley, "Guidelines for Cryptographic Key Management", BCP 107, RFC 4107, June 2005.

[RFC4442] Fries, S. and H. Tschofenig, "Bootstrapping Timed Efficient Stream Loss-Tolerant Authentication (TESLA)", RFC 4442, March 2006.

[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.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

[RFC4650] Euchner, M., "HMAC-Authenticated Diffie-Hellman for Multimedia Internet KEYing (MIKEY)", RFC 4650, September 2006.

[RFC4738] Ignjatic, D., Dondeti, L., Audet, F., and P. Lin, "MIKEY-RSA-R: An Additional Mode of Key Distribution in Multimedia Internet KEYing (MIKEY)", RFC 4738, November 2006.

[RFC5197] Fries, S. and D. Ignjatic, "On the Applicability of Various Multimedia Internet KEYing (MIKEY) Modes and Extensions", RFC 5197, June 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.

[RFC6267] Cakulev, V. and G. Sundaram, "MIKEY-IBAKE: Identity-Based Authenticated Key Exchange (IBAKE) Mode of", RFC 6267, June 2011.

Authors' Addresses

Roger K. Alexander
Cooper Power Systems
20201 Century Blvd. Suite 250
Germantown, Maryland 20874
USA

Email: roger.alexander@cooperindustries.com

Tzeta Tsao
Cooper Power Systems
20201 Century Blvd. Suite 250
Germantown, Maryland 20874
USA

Email: tzeta.tsao@cooperindustries.com