Network Working Group   F. Maino
Internet-Draft   V. Ermagan
Intended status: Standards Track   Cisco Systems
Expires: April 21, 2019   A. Cabellos
                               Universitat Politecnica de Catalunya
                                                             D. Saucez
                                                                 INRIA
                                                      October 18, 2018

                       LISP-Security (LISP-SEC)
                        draft-ietf-lisp-sec-16

Abstract

   This memo specifies LISP-SEC, a set of security mechanisms that
   provides origin authentication, integrity and anti-replay protection
   to LISP's EID-to-RLOC mapping data conveyed via mapping lookup
   process. LISP-SEC also enables verification of authorization on EID-
   prefix claims in Map-Reply messages.

Requirements Language

   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 [RFC2119].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   The Locator/ID Separation Protocol
   [I-D.ietf-lisp-rfc6830bis],[I-D.ietf-lisp-rfc6833bis] is a network-
   layer-based protocol that enables separation of IP addresses into two
   new numbering spaces: Endpoint Identifiers (EIDs) and Routing
   Locators (RLOCs). EID-to-RLOC mappings are stored in a database, the
   LISP Mapping System, and made available via the Map-Request/Map-Reply
   lookup process. If these EID-to-RLOC mappings, carried through Map-
   Reply messages, are transmitted without integrity protection, an
   adversary can manipulate them and hijack the communication,
   impersonate the requested EID, or mount Denial of Service or
   Distributed Denial of Service attacks. Also, if the Map-Reply
   message is transported unauthenticated, an adversarial LISP entity
   can overclaim an EID-prefix and maliciously redirect traffic directed
   to a large number of hosts. The LISP-SEC threat model, described in
   Section 3, is built on top of the LISP threat model defined in
   [RFC7835], that includes a detailed description of "overclaiming"
   attack.

   This memo specifies LISP-SEC, a set of security mechanisms that
   provides origin authentication, integrity and anti-replay protection
   to LISP's EID-to-RLOC mapping data conveyed via mapping lookup
   process. LISP-SEC also enables verification of authorization on EID-
   prefix claims in Map-Reply messages, ensuring that the sender of a
   Map-Reply that provides the location for a given EID-prefix is
   entitled to do so according to the EID prefix registered in the
   associated Map-Server. Map-Register security, including the right
   for a LISP entity to register an EID-prefix or to claim presence at
   an RLOC, is out of the scope of LISP-SEC. Additional security
   considerations are described in Section 6.

2. Definition of Terms

      One-Time Key (OTK): An ephemeral randomly generated key that must
      be used for a single Map-Request/Map-Reply exchange.

      ITR One-Time Key (ITR-OTK): The One-Time Key generated at the ITR.

      MS One-Time Key (MS-OTK): The One-Time Key generated at the Map-
      Server.

      Authentication Data (AD): Metadata that is included either in a
      LISP Encapsulated Control Message (ECM) header, as defined in

Section 6.1.8 of [I-D.ietf-lisp-rfc6833bis], or in a Map-Reply
message to support confidentiality, integrity protection, and
verification of EID-prefix authorization.

OTK Authentication Data (OTK-AD): The portion of ECM
Authentication Data that contains a One-Time Key.

EID Authentication Data (EID-AD): The portion of ECM and Map-Reply
Authentication Data used for verification of EID-prefix
authorization.

Packet Authentication Data (PKT-AD): The portion of Map-Reply
Authentication Data used to protect the integrity of the Map-Reply
message.

For definitions of other terms, notably Map-Request, Map-Reply,
Ingress Tunnel Router (ITR), Egress Tunnel Router (ETR), Map-Server
(MS), and Map-Resolver (MR) please consult the LISP specification
[I-D.ietf-lisp-rfc6833bis].

3. LISP-SEC Threat Model

LISP-SEC addresses the control plane threats, described in section
3.7 and 3.8 of [RFC7835], that target EID-to-RLOC mappings, including
manipulations of Map-Request and Map-Reply messages, and malicious
ETR EID prefix overclaiming. LISP-SEC makes two main assumptions:
(1) the LISP mapping system is expected to deliver a Map-Request
message to their intended destination ETR as identified by the EID,
and (2) no man-in-the-middle (MITM) attack can be mounted within the
LISP Mapping System. How the Mapping System is protected from MITM
attacks depends from the particular Mapping Systems used, and is out
of the scope of this memo. Furthermore, while LISP-SEC enables
detection of EID prefix overclaiming attacks, it assumes that Map-
Servers can verify the EID prefix authorization at time of
registration.

According to the threat model described in [RFC7835] LISP-SEC assumes
that any kind of attack, including MITM attacks, can be mounted in
the access network, outside of the boundaries of the LISP mapping
system. An on-path attacker, outside of the LISP mapping system can,
for example, hijack Map-Request and Map-Reply messages, spoofing the
identity of a LISP node. Another example of on-path attack, called
overclaiming attack, can be mounted by a malicious Egress Tunnel
Router (ETR), by overclaiming the EID-prefixes for which it is
authoritative. In this way the ETR can maliciously redirect traffic
directed to a large number of hosts.

4. **Protocol Operations**

   The goal of the security mechanisms defined in
   [I-D.ietf-lisp-rfc6833bis] is to prevent unauthorized insertion of
   mapping data by providing origin authentication and integrity
   protection for the Map-Registration, and by using the nonce to detect
   unsolicited Map-Reply sent by off-path attackers.

   LISP-SEC builds on top of the security mechanisms defined in
   [I-D.ietf-lisp-rfc6833bis] to address the threats described in
   Section 3 by leveraging the trust relationships existing among the
   LISP entities participating to the exchange of the Map-Request/Map-
   Reply messages. Those trust relationships are used to securely
   distribute a One-Time Key (OTK) that provides origin authentication,
   integrity and anti-replay protection to mapping data conveyed via the
   mapping lookup process, and that effectively prevent overclaiming
   attacks. The processing of security parameters during the Map-
   Request/Map-Reply exchange is as follows:

   o The ITR-OTK is generated and stored at the ITR, and securely
      transported to the Map-Server.

   o The Map-Server uses the ITR-OTK to compute a Keyed-Hashing for
      Message Authentication (HMAC) [RFC2104] that protects the
      integrity of the mapping data known to the Map-Server to prevent
      overclaiming attacks. The Map-Server also derives a new OTK, the
      MS-OTK, that is passed to the ETR, by applying a Key Derivation
      Function (KDF) to the ITR-OTK.

   o The ETR uses the MS-OTK to compute an HMAC that protects the
      integrity of the Map-Reply sent to the ITR.

   o Finally, the ITR uses the stored ITR-OTK to verify the integrity
      of the mapping data provided by both the Map-Server and the ETR,
      and to verify that no overclaiming attacks were mounted along the
      path between the Map-Server and the ITR.

   Section 5 provides the detailed description of the LISP-SEC control
   messages and their processing, while the rest of this section
   describes the flow of protocol operations at each entity involved in
   the Map-Request/Map-Reply exchange:

   o The ITR, upon needing to transmit a Map-Request message, generates
      and stores an OTK (ITR-OTK). This ITR-OTK is included into the
      Encapsulated Control Message (ECM) that contains the Map-Request
      sent to the Map-Resolver. To provide confidentiality to the ITR-
      OTK over the path between the ITR and its Map-Resolver, the ITR-
      OTK SHOULD be encrypted using a preconfigured key shared between

the ITR and the Map-Resolver, similar to the key shared between
the ETR and the Map-Server in order to secure ETR registration
[I-D.ietf-lisp-rfc6833bis].

o The Map-Resolver decapsulates the ECM message, decrypts the ITR-
   OTK, if needed, and forwards through the Mapping System the
   received Map-Request and the ITR-OTK, as part of a new ECM
   message. As described in Section 5.6, the LISP Mapping System
   delivers the ECM to the appropriate Map-Server, as identified by
   the EID destination address of the Map-Request.

o The Map-Server is configured with the location mappings and policy
   information for the ETR responsible for the EID destination
   address. Using this preconfigured information, the Map-Server,
   after the decapsulation of the ECM message, finds the longest
   match EID-prefix that covers the requested EID in the received
   Map-Request. The Map-Server adds this EID-prefix, together with
   an HMAC computed using the ITR-OTK, to a new Encapsulated Control
   Message that contains the received Map-Request.

o The Map-Server derives a new OTK, the MS-OTK, by applying a Key
   Derivation Function (KDF) to the ITR-OTK. This MS-OTK is included
   in the Encapsulated Control Message that the Map-Server uses to
   forward the Map-Request to the ETR. To provide MS-OTK
   confidentiality over the path between the Map-Server and the ETR,
   the MS-OTK SHOULD be encrypted using the key shared between the
   ETR and the Map-Server in order to secure ETR registration
   [I-D.ietf-lisp-rfc6833bis].

o If the Map-Server is acting in proxy mode, as specified in
   [I-D.ietf-lisp-rfc6833bis], the ETR is not involved in the
   generation of the Map-Reply. In this case the Map-Server
   generates the Map-Reply on behalf of the ETR as described below.

o The ETR, upon receiving the ECM encapsulated Map-Request from the
   Map-Server, decrypts the MS-OTK, if needed, and originates a
   standard Map-Reply that contains the EID-to-RLOC mapping
   information as specified in [I-D.ietf-lisp-rfc6833bis].

o The ETR computes an HMAC over this standard Map-Reply, keyed with
   MS-OTK to protect the integrity of the whole Map-Reply. The ETR
   also copies the EID-prefix authorization data that the Map-Server
   included in the ECM encapsulated Map-Request into the Map-Reply
   message. The ETR then sends this complete Map-Reply message to
   the requesting ITR.

o The ITR, upon receiving the Map-Reply, uses the locally stored
   ITR-OTK to verify the integrity of the EID-prefix authorization

data included in the Map-Reply by the Map-Server. The ITR
computes the MS-OTK by applying the same KDF used by the Map-
Server, and verifies the integrity of the Map-Reply. If the
integrity checks fail, the Map-Reply MUST be discarded. Also, if
the EID-prefixes claimed by the ETR in the Map-Reply are not equal
or more specific than the EID-prefix authorization data inserted
by the Map-Server, the ITR MUST discard the Map-Reply.

5. LISP-SEC Control Messages Details

LISP-SEC metadata associated with a Map-Request is transported within
the Encapsulated Control Message that contains the Map-Request.

LISP-SEC metadata associated with the Map-Reply is transported within
the Map-Reply itself.

5.1. Encapsulated Control Message LISP-SEC Extensions

LISP-SEC uses the ECM (Encapsulated Control Message) defined in
[I-D.ietf-lisp-rfc6833bis] with Type set to 8, and S bit set to 1 to
indicate that the LISP header includes Authentication Data (AD). The
format of the LISP-SEC ECM Authentication Data is defined in the
following figure. OTK-AD stands for One-Time Key Authentication Data
and EID-AD stands for EID Authentication Data.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| ECM AD Type  |V|  Reserved   |        Requested HMAC ID      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+\
|            OTK Length        |        OTK Encryption ID      | |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |
|                   One-Time-Key Preamble ...                  | |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+OTK-AD
|                 ... One-Time-Key Preamble                   | |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |
~                    One-Time Key (128 bits)                   ~/
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
|           EID-AD Length      |            KDF ID             |    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+    |
| Record Count  |   Reserved   |         EID HMAC ID           |EID-AD
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+\   |
|   Reserved    | EID mask-len |           EID-AFI             | |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Rec |
~                      EID-prefix ...                          ~ |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+/   |
~                        EID HMAC                              ~    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
```
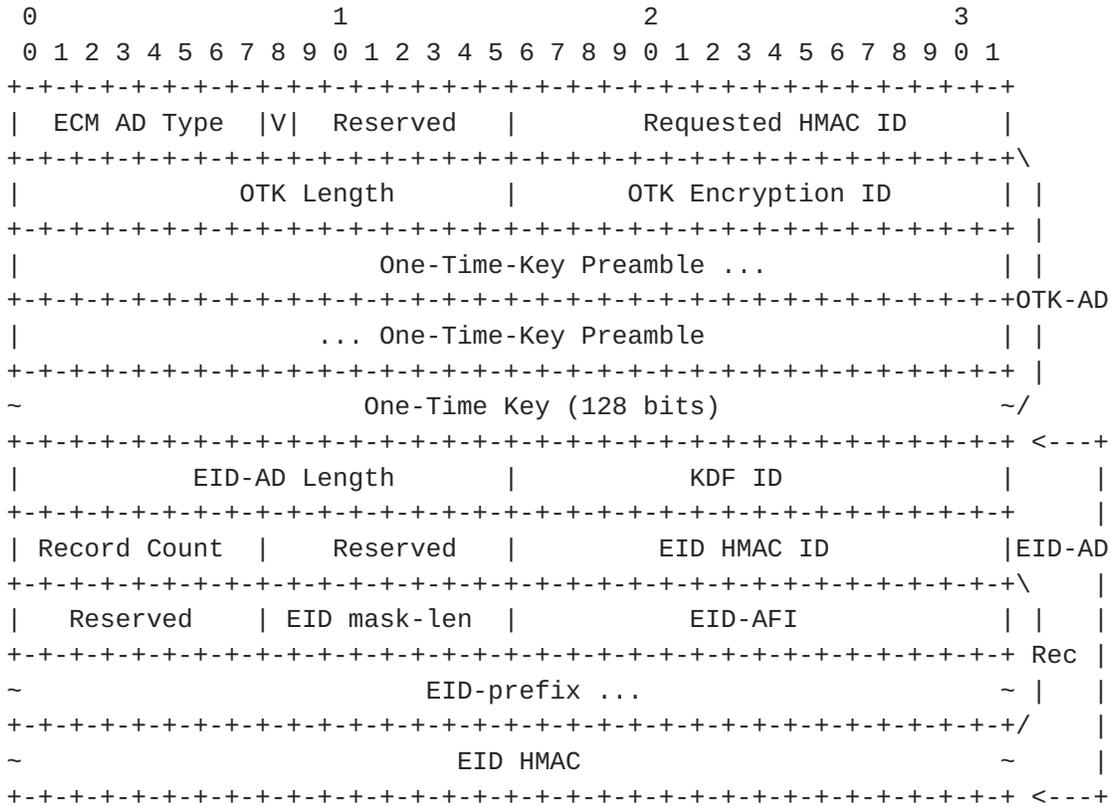
                   LISP-SEC ECM Authentication Data

     ECM AD Type: 1 (LISP-SEC Authentication Data). See Section 7.

     V: Key Version bit. This bit is toggled when the sender switches
     to a new OTK wrapping key

     Reserved: Set to 0 on transmission and ignored on receipt.

     Requested HMAC ID: The HMAC algorithm requested by the ITR. See
     Section 5.4 for details.

     OTK Length: The length (in bytes) of the OTK Authentication Data
     (OTK-AD), that contains the OTK Preamble and the OTK.

     OTK Encryption ID: The identifier of the key wrapping algorithm
     used to encrypt the One-Time-Key. When a 128-bit OTK is sent
     unencrypted by the Map-Resolver, the OTK Encryption ID is set to
     NULL_KEY_WRAP_128. See Section 5.5 for more details.

     One-Time-Key Preamble: set to 0 if the OTK is not encrypted. When
     the OTK is encrypted, this field MAY carry additional metadata
     resulting from the key wrapping operation. When a 128-bit OTK is

sent unencrypted by Map-Resolver, the OTK Preamble is set to
0x0000000000000000 (64 bits). See Section 5.5 for details.

One-Time-Key: the OTK encrypted (or not) as specified by OTK
Encryption ID. See Section 5.5 for details.

EID-AD Length: length (in bytes) of the EID Authentication Data
(EID-AD). The ITR MUST set EID-AD Length to 4 bytes, as it only
fills the KDF ID field, and all the remaining fields part of the
EID-AD are not present. An EID-AD MAY contain multiple EID-
records. Each EID-record is 4-byte long plus the length of the
AFI-encoded EID-prefix.

KDF ID: Identifier of the Key Derivation Function used to derive
the MS-OTK. The ITR MAY use this field to indicate the
recommended KDF algorithm, according to local policy. The Map-
Server can overwrite the KDF ID if it does not support the KDF ID
recommended by the ITR. See Section 5.4 for more details.

Record Count: The number of records in this Map-Request message.
A record is comprised of the portion of the packet that is labeled
'Rec' above and occurs the number of times equal to Record Count.

Reserved: Set to 0 on transmission and ignored on receipt.

EID HMAC ID: Identifier of the HMAC algorithm used to protect the
integrity of the EID-AD. This field is filled by Map-Server that
computed the EID-prefix HMAC. See Section 5.4 for more details.

EID mask-len: Mask length for EID-prefix.

EID-AFI: Address family of EID-prefix according to [RFC5226]

EID-prefix: The Map-Server uses this field to specify the EID-
prefix that the destination ETR is authoritative for, and is the
longest match for the requested EID.

EID HMAC: HMAC of the EID-AD computed and inserted by Map-Server.
Before computing the HMAC operation the EID HMAC field MUST be set
to 0. The HMAC covers the entire EID-AD.

5.2. Map-Reply LISP-SEC Extensions

LISP-SEC uses the Map-Reply defined in [I-D.ietf-lisp-rfc6833bis],
with Type set to 2, and S bit set to 1 to indicate that the Map-Reply
message includes Authentication Data (AD). The format of the LISP-
SEC Map-Reply Authentication Data is defined in the following figure.

PKT-AD is the Packet Authentication Data that covers the Map-Reply
payload.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| MR AD Type  |                 Reserved                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
|          EID-AD Length      |            KDF ID              |     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+     |
| Record Count  |   Reserved  |         EID HMAC ID         |EID-AD
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+\    |
|  Reserved   | EID mask-len  |          EID-AFI            | |   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Rec |
~                        EID-prefix ...                        ~ |   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+/    |
~                         EID HMAC                             ~    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
|          PKT-AD Length      |          PKT HMAC ID        |\
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |
~                         PKT HMAC                            ~PKT-AD
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+/
```

                   LISP-SEC Map-Reply Authentication Data

    MR AD Type: 1 (LISP-SEC Authentication Data). See Section 7.

    EID-AD Length: length (in bytes) of the EID-AD. An EID-AD MAY
    contain multiple EID-records. Each EID-record is 4-byte long plus
    the length of the AFI-encoded EID-prefix.

    KDF ID: Identifier of the Key Derivation Function used to derive
    MS-OTK. See Section 5.7 for more details.

    Record Count: The number of records in this Map-Reply message. A
    record is comprised of the portion of the packet that is labeled
    'Rec' above and occurs the number of times equal to Record Count.

    Reserved: Set to 0 on transmission and ignored on receipt.

    EID HMAC ID: Identifier of the HMAC algorithm used to protect the
    integrity of the EID-AD. See Section 5.7 for more details.

    EID mask-len: Mask length for EID-prefix.

    EID-AFI: Address family of EID-prefix according to [RFC5226].

EID-prefix: This field contains an EID-prefix that the destination
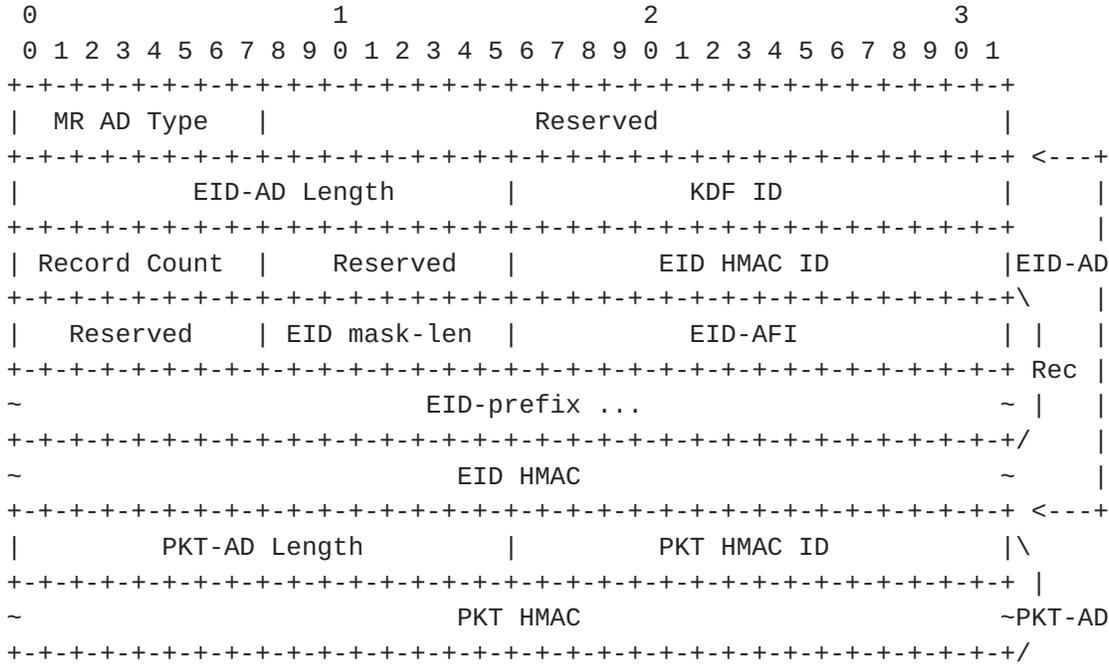ETR is authoritative for, and is the longest match for the
requested EID.

EID HMAC: HMAC of the EID-AD, as computed by the Map-Server.
Before computing the HMAC operation the EID HMAC field MUST be set
to 0. The HMAC covers the entire EID-AD.

PKT-AD Length: length (in bytes) of the Packet Authentication Data
(PKT-AD).

PKT HMAC ID: Identifier of the HMAC algorithm used to protect the
integrity of the Map-reply.

PKT HMAC: HMAC of the whole Map-Reply packet, including the LISP-
SEC Authentication Data. The scope of the authentication goes
from the Map-Reply Type field to the PKT HMAC field included.
Before computing the HMAC operation the PKT HMAC field MUST be set
to 0. See Section 5.8 for more details.

5.3. Map-Register LISP-SEC Extentions

This memo is allocating one of the bits marked as Reserved in the
Map-Register message defined in Section 6.1.6 of
[I-D.ietf-lisp-rfc6833bis]. More precisely, the second bit after the
Type field in a Map-Register message is allocated as the S bit. The
S bit indicates to the Map-Server that the registering ETR is LISP-
SEC enabled. An ETR that supports LISP-SEC MUST set the S bit in its
Map-Register messages.

5.4. ITR Processing

Upon creating a Map-Request, the ITR generates a random ITR-OTK that
is stored locally, together with the nonce generated as specified in
[I-D.ietf-lisp-rfc6833bis].

The Map-Request MUST be encapsulated in an ECM, with the S-bit set to
1, to indicate the presence of Authentication Data. If the ITR and
the Map-Resolver are configured with a shared key, the ITR-OTK
confidentiality SHOULD be protected by wrapping the ITR-OTK with the
algorithm specified by the OTK Encryption ID field. See Section 5.5
for further details on OTK encryption.

The Requested HMAC ID field contains the suggested HMAC algorithm to
be used by the Map-Server and the ETR to protect the integrity of the
ECM Authentication data and of the Map-Reply.

The KDF ID field specifies the suggested key derivation function to
be used by the Map-Server to derive the MS-OTK. A KDF Value of NONE
(0), MAY be used to specify that the ITR has no preferred KDF ID.

The EID-AD length is set to 4 bytes, since the Authentication Data
does not contain EID-prefix Authentication Data, and the EID-AD
contains only the KDF ID field.

In response to an encapsulated Map-Request that has the S-bit set, an
ITR MUST receive a Map-Reply with the S-bit set, that includes an
EID-AD and a PKT-AD. If the Map-Reply does not include both ADs, the
ITR MUST discard it. In response to an encapsulated Map-Request with
S-bit set to 0, the ITR expects a Map-Reply with S-bit set to 0, and
the ITR SHOULD discard the Map-Reply if the S-bit is set.

Upon receiving a Map-Reply, the ITR must verify the integrity of both
the EID-AD and the PKT-AD, and MUST discard the Map-Reply if one of
the integrity checks fails. After processing the Map-Reply, the ITR
must discard the <nonce,ITK-OTK> pair associated to the Map-Reply

The integrity of the EID-AD is verified using the locally stored ITR-
OTK to re-compute the HMAC of the EID-AD using the algorithm
specified in the EID HMAC ID field. If the EID HMAC ID field does
not match the Requested HMAC ID the ITR SHOULD discard the Map-Reply
and send, at the first opportunity it needs to, a new Map-Request
with a different Requested HMAC ID field, according to ITR's local
policy. The scope of the HMAC operation covers the entire EID-AD,
from the EID-AD Length field to the EID HMAC field, which must be set
to 0 before the computation of the HMAC.

ITR MUST set the EID HMAC ID field to 0 before computing the HMAC.

To verify the integrity of the PKT-AD, first the MS-OTK is derived
from the locally stored ITR-OTK using the algorithm specified in the
KDF ID field. This is because the PKT-AD is generated by the ETR
using the MS-OTK. If the KDF ID in the Map-Reply does not match the
KDF ID requested in the Map-Request, the ITR SHOULD discard the Map-
Reply and send, at the first opportunity it needs to, a new Map-
Request with a different KDF ID, according to ITR's local policy.

The derived MS-OTK is then used to re-compute the HMAC of the PKT-AD
using the Algorithm specified in the PKT HMAC ID field. If the PKT
HMAC ID field does not match the Requested HMAC ID the ITR SHOULD
discard the Map-Reply and send, at the first opportunity it needs to,
a new Map-Request with a different Requested HMAC ID according to
ITR's local policy or until all HMAC IDs supported by the ITR have
been attempted.

Each individual Map-Reply EID-record is considered valid only if: (1)
both EID-AD and PKT-AD are valid, and (2) the intersection of the
EID-prefix in the Map-Reply EID-record with one of the EID-prefixes
contained in the EID-AD is not empty. After identifying the Map-
Reply record as valid, the ITR sets the EID-prefix in the Map-Reply
record to the value of the intersection set computed before, and adds
the Map-Reply EID-record to its EID-to-RLOC cache, as described in
[I-D.ietf-lisp-rfc6833bis]. An example of Map-Reply record
validation is provided in Section 5.4.1.

The ITR SHOULD send SMR triggered Map-Requests over the mapping
system in order to receive a secure Map-Reply. If an ITR accepts
piggybacked Map-Replies, it SHOULD also send a Map-Request over the
mapping system in order to verify the piggybacked Map-Reply with a
secure Map-Reply.

5.4.1. Map-Reply Record Validation

The payload of a Map-Reply may contain multiple EID-records. The
whole Map-Reply is signed by the ETR, with the PKT HMAC, to provide
integrity protection and origin authentication to the EID-prefix
records claimed by the ETR. The Authentication Data field of a Map-
Reply may contain multiple EID-records in the EID-AD. The EID-AD is
signed by the Map-Server, with the EID HMAC, to provide integrity
protection and origin authentication to the EID-prefix records
inserted by the Map-Server.

Upon receiving a Map-Reply with the S-bit set, the ITR first checks
the validity of both the EID HMAC and of the PKT-AD HMAC. If either
one of the HMACs is not valid, a log action MUST be taken and the
Map-Reply MUST NOT be processed any further. If both HMACs are
valid, the ITR proceeds with validating each individual EID-record
claimed by the ETR by computing the intersection of each one of the
EID-prefix contained in the payload of the Map-Reply with each one of
the EID-prefixes contained in the EID-AD. An EID-record is valid
only if at least one of the intersections is not the empty set.

For instance, the Map-Reply payload contains 3 mapping record EID-
prefixes:

    2001:db8:0102::/48

    2001:db8:0103::/48

    2001:db8:0200::/40

The EID-AD contains two EID-prefixes:

    2001:db8:0103::/48

    2001:db8:0203::/48

   The EID-record with EID-prefix 2001:db8:0102::/48 is not eligible to
   be used by the ITR since it is not included in any of the EID-ADs
   signed by the Map-Server. A log action MUST be taken.

   The EID-record with EID-prefix 2001:db8:0103::/48 is eligible to be
   used by the ITR because it matches the second EID-prefix contained in
   the EID-AD.

   The EID-record with EID-prefix 2001:db8:0200::/40 is not eligible to
   be used by the ITR since it is not included in any of the EID-ADs
   signed by the Map-Server. A log action MUST be taken. In this last
   example the ETR is trying to over claim the EID-prefix
   2001:db8:0200::/40, but the Map-Server authorized only
   2001:db8:0203::/48, hence the EID-record is discarded.

5.4.2. PITR Processing

   The processing performed by a PITR is equivalent to the processing of
   an ITR. However, if the PITR is directly connected to a Mapping
   System such as LISP+ALT [RFC6836], the PITR performs the functions of
   both the ITR and the Map-Resolver forwarding the Map-Request
   encapsulated in an ECM header that includes the Authentication Data
   fields as described in Section 5.6.

5.5. Encrypting and Decrypting an OTK

   MS-OTK confidentiality is required in the path between the Map-Server
   and the ETR, the MS-OTK SHOULD be encrypted using the preconfigured
   key shared between the Map-Server and the ETR for the purpose of
   securing ETR registration [I-D.ietf-lisp-rfc6833bis]. Similarly, if
   ITR-OTK confidentiality is required in the path between the ITR and
   the Map-Resolver, the ITR-OTK SHOULD be encrypted with a key shared
   between the ITR and the Map-Resolver.

   The OTK is encrypted using the algorithm specified in the OTK
   Encryption ID field. When the AES Key Wrap algorithm is used to
   encrypt a 128-bit OTK, according to [RFC3394], the AES Key Wrap
   Initialization Value MUST be set to 0xA6A6A6A6A6A6A6A6 (64 bits).
   The output of the AES Key Wrap operation is 192-bit long. The most
   significant 64-bit are copied in the One-Time Key Preamble field,
   while the 128 less significant bits are copied in the One-Time Key
   field of the LISP-SEC Authentication Data.

When decrypting an encrypted OTK the receiver MUST verify that the
Initialization Value resulting from the AES Key Wrap decryption
operation is equal to 0xA6A6A6A6A6A6A6A6. If this verification fails
the receiver MUST discard the entire message.

When a 128-bit OTK is sent unencrypted the OTK Encryption ID is set
to NULL_KEY_WRAP_128, and the OTK Preamble is set to
0x0000000000000000 (64 bits).

5.6. Map-Resolver Processing

Upon receiving an encapsulated Map-Request with the S-bit set, the
Map-Resolver decapsulates the ECM message. The ITR-OTK, if
encrypted, is decrypted as specified in Section 5.5.

Protecting the confidentiality of the ITR-OTK and, in general, the
security of how the Map-Request is handed by the Map-Resolver to the
Map-Server, is specific to the particular Mapping System used, and
outside of the scope of this memo.

In Mapping Systems where the Map-Server is compliant with
[I-D.ietf-lisp-rfc6833bis], the Map-Resolver originates a new ECM
header with the S-bit set, that contains the unencrypted ITR-OTK, as
specified in Section 5.5, and the other data derived from the ECM
Authentication Data of the received encapsulated Map-Request.

The Map-Resolver then forwards to the Map-Server the received Map-
Request, encapsulated in the new ECM header that includes the newly
computed Authentication Data fields.

5.7. Map-Server Processing

Upon receiving an ECM encapsulated Map-Request with the S-bit set,
the Map-Server process the Map-Request according to the value of the
S-bit contained in the Map-Register sent by the ETR during
registration.

If the S-bit contained in the Map-Register was clear the Map-Server
decapsulates the ECM and generates a new ECM encapsulated Map-Request
that does not contain an ECM Authentication Data, as specified in
[I-D.ietf-lisp-rfc6833bis]. The Map-Server does not perform any
further LISP-SEC processing, and the Map-Reply will not be protected.

If the S-bit contained in the Map-Register was set the Map-Server
decapsulates the ECM and generates a new ECM Authentication Data.
The Authentication Data includes the OTK-AD and the EID-AD, that
contains EID-prefix authorization information, that are ultimately
sent to the requesting ITR.

The Map-Server updates the OTK-AD by deriving a new OTK (MS-OTK) from
the ITR-OTK received with the Map-Request. MS-OTK is derived
applying the key derivation function specified in the KDF ID field.
If the algorithm specified in the KDF ID field is not supported, the
Map-Server uses a different algorithm to derive the key and updates
the KDF ID field accordingly.

The Map-Server and the ETR MUST be configured with a shared key for
mapping registration according to [I-D.ietf-lisp-rfc6833bis]. If MS-
OTK confidentiality is required, then the MS-OTK SHOULD be encrypted,
by wrapping the MS-OTK with the algorithm specified by the OTK
Encryption ID field as specified in Section 5.5.

The Map-Server includes in the EID-AD the longest match registered
EID-prefix for the destination EID, and an HMAC of this EID-prefix.
The HMAC is keyed with the ITR-OTK contained in the received ECM
Authentication Data, and the HMAC algorithm is chosen according to
the Requested HMAC ID field. If The Map-Server does not support this
algorithm, the Map-Server uses a different algorithm and specifies it
in the EID HMAC ID field. The scope of the HMAC operation covers the
entire EID-AD, from the EID-AD Length field to the EID HMAC field,
which must be set to 0 before the computation.

The Map-Server then forwards the updated ECM encapsulated Map-
Request, that contains the OTK-AD, the EID-AD, and the received Map-
Request to an authoritative ETR as specified in
[I-D.ietf-lisp-rfc6833bis].

5.7.1. Map-Server Processing in Proxy mode

If the Map-Server is in proxy mode, it generates a Map-Reply, as
specified in [I-D.ietf-lisp-rfc6833bis], with the S-bit set to 1.
The Map-Reply includes the Authentication Data that contains the EID-
AD, computed as specified in Section 5.7, as well as the PKT-AD
computed as specified in Section 5.8.

5.8. ETR Processing

Upon receiving an ECM encapsulated Map-Request with the S-bit set,
the ETR decapsulates the ECM message. The OTK field, if encrypted,
is decrypted as specified in Section 5.5 to obtain the unencrypted
MS-OTK.

The ETR then generates a Map-Reply as specified in
[I-D.ietf-lisp-rfc6833bis] and includes the Authentication Data that
contains the EID-AD, as received in the encapsulated Map-Request, as
well as the PKT-AD.

The EID-AD is copied from the Authentication Data of the received
encapsulated Map-Request.

The PKT-AD contains the HMAC of the whole Map-Reply packet, keyed
with the MS-OTK and computed using the HMAC algorithm specified in
the Requested HMAC ID field of the received encapsulated Map-Request.
If the ETR does not support the Requested HMAC ID, it uses a
different algorithm and updates the PKT HMAC ID field accordingly.
The scope of the HMAC operation covers the entire PKT-AD, from the
Map-Reply Type field to the PKT HMAC field, which must be set to 0
before the computation.

Finally the ETR sends the Map-Reply to the requesting ITR as
specified in [I-D.ietf-lisp-rfc6833bis].

6. Security Considerations

6.1. Mapping System Security

The LISP-SEC threat model described in Section 3, assumes that the
LISP Mapping System is working properly and eventually delivers Map-
Request messages to a Map-Server that is authoritative for the
requested EID.

It is assumed that the Mapping System ensures the confidentiality of
the OTK, and the integrity of the Map-Reply data. However, how the
LISP Mapping System is secured is out of the scope of this document.

Similarly, Map-Register security, including the right for a LISP
entity to register an EID-prefix or to claim presence at an RLOC, is
out of the scope of LISP-SEC.

6.2. Random Number Generation

The ITR-OTK MUST be generated by a properly seeded pseudo-random (or
strong random) source. See [RFC4086] for advice on generating
security-sensitive random data

6.3. Map-Server and ETR Colocation

If the Map-Server and the ETR are colocated, LISP-SEC does not
provide protection from overclaiming attacks mounted by the ETR.
However, in this particular case, since the ETR is within the trust
boundaries of the Map-Server, ETR's overclaiming attacks are not
included in the threat model.

6.4. Deploying LISP-SEC

   This memo is written according to [RFC2119]. Specifically, the use
   of the key word SHOULD "or the adjective 'RECOMMENDED', mean that
   there may exist valid reasons in particular circumstances to ignore a
   particular item, but the full implications must be understood and
   carefully weighed before choosing a different course".

   Those deploying LISP-SEC according to this memo, should carefully
   weight how the LISP-SEC threat model applies to their particular use
   case or deployment. If they decide to ignore a particular
   recommendation, they should make sure the risk associated with the
   corresponding threats is well understood.

   As an example, in certain closed and controlled deployments, it is
   possible that the threat associated with a MiTM between the xTR and
   the Mapping System is very low, and after carfeul consideration it
   may be decided to allow a NULL key wrapping algorithm while carrying
   the OTKs between the xTR and the Mapping System.

   As an example at the other end of the spectrum, in certain other
   deployments, attackers may be very sophisticated, and force the
   deployers to enforce very strict policies in term of HMAC algorithms
   accepted by an ITR.

   Similar considerations apply to the entire LISP-SEC threat model, and
   should guide the deployers and implementors whenever they encounter
   the key word SHOULD across this memo.

6.5. Shared Keys Provisioning

   Provisioning of the keys shared between the ITR and the Map-Resolver
   as well as between the ETR and the Map-Server should be performed via
   an orchestration infrastructure and it is out of the scope of this
   draft. It is recommended that both shared keys are refreshed at
   periodical intervals to address key aging or attackers gaining
   unauthorized access to the shared keys. Shared keys should be
   unpredictable random values.

6.6. Replay Attacks

   An attacker can capture a valid Map-Request and/or Map-Reply and
   replay it, however once the ITR receives the original Map-Reply the
   <nonce,ITR-OTK> pair stored at the ITR will be discarded. If a
   replayed Map-Reply arrives at the ITR, there is no <nonce,ITR-OTK>
   that matches the incoming Map-Reply and will be discarded.

In case of replayed Map-Request, the Map-Server, Map-Resolver and ETR
will have to do a LISP-SEC computation. This is equivalent to a
valid LISP-SEC computation and an attacker does not obtain any
benefit.

6.7. Denial of Service and Distributed Denial of Service Attacks

LISP-SEC mitigates the risks of Denial of Service and Distributed
Denial of Service attacks by protecting the integrity and
authenticating the origin of the Map-Request/Map-Reply messages, and
by preventing malicious ETRs from overclaiming EID prefixes that
could re-direct traffic directed to a potentially large number of
hosts.

7. IANA Considerations

7.1. ECM AD Type Registry

IANA is requested to create the "ECM Authentication Data Type"
registry with values 0-255, for use in the ECM LISP-SEC Extensions
Section 5.1. The registry MUST be initially populated with the
following values:

Name	Value	Defined In
Reserved	0	This memo
LISP-SEC-ECM-EXT	1	This memo

                         HMAC Functions

Values 2-255 are unassigned. They are to be assigned according to
the "Specification Required" policy defined in [RFC5226].

7.2. Map-Reply AD Type Registry

IANA is requested to create the "Map-Reply Authentication Data Type"
registry with values 0-255, for use in the Map-Reply LISP-SEC
Extensions Section 5.2. The registry MUST be initially populated
with the following values:

Name	Value	Defined In
Reserved	0	This memo
LISP-SEC-MR-EXT	1	This memo

                         HMAC Functions

Values 2-255 are unassigned. They are to be assigned according to
the "Specification Required" policy defined in [RFC5226].

7.3. HMAC Functions

IANA is requested to create the "LISP-SEC Authentication Data HMAC
ID" registry with values 0-65535 for use as Requested HMAC ID, EID
HMAC ID, and PKT HMAC ID in the LISP-SEC Authentication Data:

Name	Number	Defined In
NONE	0	This memo
AUTH-HMAC-SHA-1-96	1	[RFC2104]
AUTH-HMAC-SHA-256-128	2	[RFC6234]

HMAC Functions

Values 3-65535 are unassigned. They are to be assigned according to
the "Specification Required" policy defined in [RFC5226].

AUTH-HMAC-SHA-1-96 MUST be supported, AUTH-HMAC-SHA-256-128 SHOULD be
supported.

7.4. Key Wrap Functions

IANA is requested to create the "LISP-SEC Authentication Data Key
Wrap ID" registry with values 0-65535 for use as OTK key wrap
algorithms ID in the LISP-SEC Authentication Data:

Name	Number	Defined In
Reserved	0	This memo
NULL-KEY-WRAP-128	1	This memo
AES-KEY-WRAP-128	2	[RFC3394]

Key Wrap Functions

Values 3-65535 are unassigned. They are to be assigned according to
the "Specification Required" policy defined in [RFC5226].

NULL-KEY-WRAP-128, and AES-KEY-WRAP-128 MUST be supported.

NULL-KEY-WRAP-128 is used to carry an unencrypted 128-bit OTK, with a
64-bit preamble set to 0x0000000000000000 (64 bits).

7.5. Key Derivation Functions

   IANA is requested to create the "LISP-SEC Authentication Data Key
   Derivation Function ID" registry with values 0-65535 for use as KDF
   ID in the LISP-SEC Authentication Data:

```
             Name                       Number       Defined In
             --------------------------------------------------
             NONE                         0           This memo
             HKDF-SHA1-128                1           [RFC5869]
```

                        Key Derivation Functions

   Values 2-65535 are unassigned. They are to be assigned according to
   the "Specification Required" policy defined in [RFC5226].

   HKDF-SHA1-128 MUST be supported

8. Acknowledgements

   The authors would like to acknowledge Pere Monclus, Dave Meyer, Dino
   Farinacci, Brian Weis, David McGrew, Darrel Lewis and Landon Curt
   Noll for their valuable suggestions provided during the preparation
   of this document.

9. Normative References

   [I-D.ietf-lisp-rfc6830bis]
            Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A.
            Cabellos-Aparicio, "The Locator/ID Separation Protocol
            (LISP)", draft-ietf-lisp-rfc6830bis-24 (work in progress),
            October 2018.

   [I-D.ietf-lisp-rfc6833bis]
            Fuller, V., Farinacci, D., and A. Cabellos-Aparicio,
            "Locator/ID Separation Protocol (LISP) Control-Plane",
            draft-ietf-lisp-rfc6833bis-18 (work in progress), October
            2018.

   [RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-
            Hashing for Message Authentication", RFC 2104,
            DOI 10.17487/RFC2104, February 1997, <https://www.rfc-
            editor.org/info/rfc2104>.

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119,
               DOI 10.17487/RFC2119, March 1997, <https://www.rfc-
               editor.org/info/rfc2119>.

   [RFC3394]   Schaad, J. and R. Housley, "Advanced Encryption Standard
               (AES) Key Wrap Algorithm", RFC 3394, DOI 10.17487/RFC3394,
               September 2002, <https://www.rfc-editor.org/info/rfc3394>.

   [RFC4086]   Eastlake 3rd, D., Schiller, J., and S. Crocker,
               "Randomness Requirements for Security", BCP 106, RFC 4086,
               DOI 10.17487/RFC4086, June 2005, <https://www.rfc-
               editor.org/info/rfc4086>.

   [RFC5226]   Narten, T. and H. Alvestrand, "Guidelines for Writing an
               IANA Considerations Section in RFCs", RFC 5226,
               DOI 10.17487/RFC5226, May 2008, <https://www.rfc-
               editor.org/info/rfc5226>.

   [RFC5869]   Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand
               Key Derivation Function (HKDF)", RFC 5869,
               DOI 10.17487/RFC5869, May 2010, <https://www.rfc-
               editor.org/info/rfc5869>.

   [RFC6234]   Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms
               (SHA and SHA-based HMAC and HKDF)", RFC 6234,
               DOI 10.17487/RFC6234, May 2011, <https://www.rfc-
               editor.org/info/rfc6234>.

   [RFC6836]   Fuller, V., Farinacci, D., Meyer, D., and D. Lewis,
               "Locator/ID Separation Protocol Alternative Logical
               Topology (LISP+ALT)", RFC 6836, DOI 10.17487/RFC6836,
               January 2013, <https://www.rfc-editor.org/info/rfc6836>.

   [RFC7835]   Saucez, D., Iannone, L., and O. Bonaventure, "Locator/ID
               Separation Protocol (LISP) Threat Analysis", RFC 7835,
               DOI 10.17487/RFC7835, April 2016, <https://www.rfc-
               editor.org/info/rfc7835>.

Authors' Addresses

   Fabio Maino
   Cisco Systems
   170 Tasman Drive
   San Jose, California 95134
   USA

   Email: fmaino@cisco.com

   Vina Ermagan
   Cisco Systems
   170 Tasman Drive
   San Jose, California 95134
   USA

   Email: vermagan@cisco.com

   Albert Cabellos
   Universitat Politecnica de Catalunya
   c/ Jordi Girona s/n
   Barcelona 08034
   Spain

   Email: acabello@ac.upc.edu

   Damien Saucez
   INRIA
   2004 route des Lucioles - BP 93
   Sophia Antipolis
   France

   Email: damien.saucez@inria.fr