Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 8, 2023

F. Maino
Cisco Systems
V. Ermagan
Google
A. Cabellos
Universitat Politecnica de Catalunya
D. Saucez
Inria

July 7, 2022

LISP-Security (LISP-SEC)
draft-ietf-lisp-sec-29

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 the mapping lookup process. LISP-SEC also enables verification of authorization on EID-prefix claims in Map-Reply messages.

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. The LISP-SEC threat model, described in Section 4, 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/Map-Notify 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 as those protocols are protected by the security mechanisms specified in [I-D.ietf-lisp-rfc6833bis]. However, LISP-SEC extends the Map-Register message to allow an ITR to downgrade to non LISP-SEC Map-Requests. Additional security considerations are described in Section 6.

2. Requirements Notation

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. 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 Ingress Tunnel Router (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 [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].

4. 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 on-path attack can be mounted within the LISP Mapping System. How the Mapping System is protected from on-path attacks depends from the particular Mapping System 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 registration time.

According to the threat model described in [RFC7835] LISP-SEC assumes that any kind of attack, including on-path attacks, can be mounted 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.

5. 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-Register, 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 to address the threats described in Section 4 by leveraging the trust relationships existing among the LISP entities ([I-D.ietf-lisp-rfc6833bis]) participating in the exchange of the Map-Request/Map-Reply messages. Those trust relationships (see also Section 7 and [I-D.ietf-lisp-rfc6833bis]) are used to securely distribute, as described in Section 8.4, a per-message 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 Per each Map-Request message a new 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) (e.g. [RFC5869]) 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 6 provides the detailed description of the LISP-SEC control messages and their processing, while the rest of this section describes the flow of LISP protocol operations at each entity involved in the Map-Request/Map-Reply exchange:

1. The ITR, upon needing to transmit a Map-Request message, generates and stores an OTK (ITR-OTK). This ITR-OTK is encrypted and included into the Encapsulated Control Message (ECM) that contains the Map-Request sent to the Map-Resolver.

2. 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. The LISP Mapping System delivers the ECM to the appropriate Map-Server, as identified by the EID destination address of the Map-Request.

3. 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.

4. 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.

5. 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 and steps 6 and 7 are skipped. In this case the Map-Server generates the Map-Reply on behalf of the ETR as described in Section 6.7.2.

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

7. The ETR computes an HMAC over the 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 the complete Map-Reply message to the requesting ITR.

8. 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 (as specified in the ECM encapsulated Map-Reply) used by the Map-Server, and verifies the integrity of the Map-Reply.

6. 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.

These specifications use Keyed-Hashing for Message Authentication (HMAC) in various places (as described in the following). The HMAC function AUTH-HMAC-SHA-256-128 [RFC6234] MUST be supported in LISP-SEC implementations. LISP-SEC deployments SHOULD use AUTH-HMAC-SHA-256-128 HMAC function, except when communicating with older implementations that only support AUTH-HMAC-SHA-1-96 [RFC2104].

6.1. Encapsulated Control Message LISP-SEC Extensions

LISP-SEC uses the ECM defined in [I-D.ietf-lisp-rfc6833bis] with 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 Figure 1 . 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  |   Unassigned  |        Requested HMAC ID      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+\
   |              OTK Length       |     Key ID    | OTK Wrap. ID  | |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |
   |                       One-Time-Key Preamble ...               | |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+OTK-AD
   |                   ... One-Time-Key Preamble                   | |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |
   ~                      One-Time Key (128 bits)                  ~/
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
   |           EID-AD Length       |           KDF ID              |     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+     |
   | Record Count  |E| Unassigned  |         EID HMAC ID           |EID-AD
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+\    |
   |  Unassigned   | EID mask-len  |           EID-AFI             | |   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Rec |
   ~                          EID-prefix ...                       ~ |   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+/    |
   ~                            EID HMAC                           ~     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
```

Figure 1: LISP-SEC ECM Authentication Data

ECM AD Type: 1 (LISP-SEC Authentication Data). See Section 8.

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

Requested HMAC ID: The HMAC algorithm, that will be used to protect the mappings, requested by the ITR. Permitted values are registered in the LISP-SEC Authentication Data HMAC ID (see Section 8.3). Refer to Section 6.4 for more details.

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

Key ID: The identifier of the pre-shared secret shared by an ITR and the Map-Resolver, and by the Map-Server and an ETR. Per-message keys are derived from the pre-shared secret to encrypt, authenticate the origin and protect the integrity of the OTK. The Key ID allows to rotate between multiple pre-shared secrets in a non disruptive way.

OTK Wrapping ID (OTK Wrap. ID): The identifier of the key derivation function and of the key wrapping algorithm used to encrypt the One-Time-Key. Permitted values are registered in the

LISP-SEC Authentication Data Key Wrap ID (see Section 8.4). Refer to Section 6.5 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 a Map-Resolver, the OTK Preamble is set to 0x0000000000000000 (64 bits). See Section 6.5.1 for details.

One-Time-Key: the OTK wrapped as specified by OTK Wrapping ID. See Section 6.5 for details.

EID-AD Length: length (in bytes) of the EID Authentication Data (EID-AD). The ITR MUST set the 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. Permitted values are registered in the LISP-SEC Authentication Data Key Derivation Function ID (see Section 8.5). Refer to Section 6.7 for more details.

Record Count: As defined in Section 5.2 of [I-D.ietf-lisp-rfc6833bis].

E: ETR-Cant-Sign bit. If this bit is set to 1, it signals to the ITR that at least one of the ETRs authoritative for the EID prefixes of this Map-Reply has not enabled LISP-SEC. Only a Map-Server can set this bit. See Section 6.7 for more details.

Unassigned: 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 the Map-Server that computed the EID-prefix HMAC. See Section 6.7.1 for more details.

EID mask-len: As defined in Section 5.2 of [I-D.ietf-lisp-rfc6833bis].

EID-AFI: As defined in Section 5.2 of [I-D.ietf-lisp-rfc6833bis].

EID-prefix: As defined in Section 5.2 of [I-D.ietf-lisp-rfc6833bis].

EID HMAC: HMAC of the EID-AD computed and inserted by a Map-Server See Section 6.7.1 for more details.

6.2. 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 Figure 2. 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   |                 Unassigned                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
|           EID-AD Length       |           KDF ID              |     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+     |
| Record Count  |  Unassigned   |         EID HMAC ID           |EID-AD
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+\    |
|  Unassigned   | EID mask-len  |           EID-AFI             | |   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Rec |
~                          EID-prefix ...                       ~ |   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+/    |
~                            EID HMAC                           ~     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ <---+
|         PKT-AD Length         |         PKT HMAC ID           |\
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |
~                            PKT HMAC                           ~PKT-AD
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+/
```

Figure 2: LISP-SEC Map-Reply Authentication Data

MR AD Type: 1 (LISP-SEC Authentication Data). See Section 8.

EID-AD Length: length (in bytes) of the EID-AD (see Section 6.1).

KDF ID: Identifier of the Key Derivation Function used to derive MS-OTK (see Section 6.1).

Record Count: The number of records in this Map-Reply message (see Section 6.1).

Unassigned: 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 6.1).

EID mask-len: Mask length for EID-prefix (see Section 6.1).

EID-AFI: See Section 6.1. .

EID-prefix: See Section 6.1.

EID HMAC: See Section 6.1.

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 (see Section 6.5).

PKT HMAC: HMAC of the whole Map-Reply packet, so to protect its integrity; including the LISP-SEC Authentication Data (from the Map-Reply Type field to the PKT HMAC field), which allow message authetification.

6.3. Map-Register LISP-SEC Extensions

The S bit in the Map-Register message (see [I-D.ietf-lisp-rfc6833bis]) 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.

6.4. ITR Processing: Generating a Map-Request

Upon creating a Map-Request, the ITR generates a random ITR-OTK that is stored locally, until the corresponding Map-Reply is received (see Section 6.9), together with the nonce generated as specified in [I-D.ietf-lisp-rfc6833bis].

The ITR MAY use the KDF ID 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 6.7). A KDF value of NOPREF (0) may be used to specify that the ITR has no preferred KDF ID.

ITR-OTK confidentiality and integrity protection MUST be provided in the path between the ITR and the Map-Resolver. This can be achieved either by encrypting the ITR-OTK with the pre-shared secret known to the ITR and the Map-Resolver (see Section 6.5), or by enabling DTLS [RFC9147] between the ITR and the Map-Resolver.

The Map-Request (as defined in [I-D.ietf-lisp-rfc6833bis]) MUST be encapsulated as a LISP Control Message in an ECM, with the S-bit set to 1, to indicate the presence of Authentication Data. Such a message is also called "Protected Map-Request" in this memo.

The ITR-OTK is wrapped with the algorithm specified by the OTK Wrapping ID field. See Section 6.5 for further details on OTK encryption. If the NULL-KEY-WRAP-128 algorithm (see Section 8.4) is selected, and no other encryption mechanism (e.g. DTLS) is enabled in the path between the ITR and the Map-Resolver, the Map-Request MUST be dropped, and an appropriate log action SHOULD be taken. Implementations may include mechanisms (which are beyond the scope of this document) to avoid log resource exhaustion attacks.

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. A HMAC ID Value of NONE (0), MAY be used to specify that the ITR has no preferred HMAC ID.

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.

If the ITR is directly connected to a Mapping System, such as LISP+ALT [RFC6836], it performs the functions of both the ITR and the Map-Resolver, forwarding the Protected Map-Request as described in Section 6.6.

The processing performed by Proxy ITRs (PITRs) is equivalent to the processing of an ITR, hence the procedure described above applies.

6.5. Encrypting and Decrypting an OTK

MS-OTK confidentiality and integrity protection MUST be provided in the path between the Map-Server and the ETR. This can be achieved either by enabling DTLS between the Map-Server and the ETR or by encrypting the MS-OTK with the pre-shared secret known to the Map-Server and the ETR [I-D.ietf-lisp-rfc6833bis].

Similarly, ITR-OTK confidentiality and integrity protection MUST be provided in the path between the ITR and the Map-Resolver. This can be achieved either by enabling DTLS between the Map-Server and the ITR, or by encrypting the ITR-OTK with the pre-shared secret known to the ITR and the Map-Resolver. The ITR/Map-Resolver pre-shared key is similar to the Map-Server/ETR pre-shared key.

This section describes OTK processing in the ITR/Map-Resolver path, as well as in the Map-Server/ETR path.

It's important to note that, to prevent ETR's overclaiming attacks, the ITR/Map-Resolver pre-shared secret MUST be independent from the Map-Server/ETR pre-shared secret.

The OTK is wrapped using the algorithm specified in the OTK Wrapping ID field. This field identifies both the:

- o Key Encryption Algorithm used to encrypt the wrapped OTK.
- o Key Derivation Function used to derive a per-message encryption key.

Implementations of this specification MUST support OTK Wrapping ID AES-KEY-WRAP-128+HKDF-SHA256 that specifies the use of the HKDF-SHA256 Key Derivation Function specified in [RFC5869] to derive a per-message encryption key (per-msg-key), as well as the AES-KEY-WRAP-128 Key Wrap algorithm used to encrypt a 128-bit OTK, according to [RFC3394].

Implementations of this specification MUST support OTK Wrapping NULL-KEY-WRAP-128. NULL-KEY-WRAP-128 is used to carry an unencrypted 128-bit OTK, with a 64-bit preamble set to 0x0000000000000000 (64 bits).

The key wrapping process for OTK Wrapping ID AES-KEY-WRAP-128+HKDF-SHA256 is described below:

1. The KDF and Key Wrap algorithms are identified by the value of the 'OTK Wrapping ID' field. The initial values are documented in Table 5.

2. If the NULL-KEY-WRAP-128 algorithm (see Section 8.4) is selected and DTLS is not enabled, the Map-Request MUST be dropped and an appropriate log action SHOULD be taken. Implementations may include mechanisms (which are beyond the scope of this document) to avoid log resource exhaustion attacks.

3. The pre-shared secret used to derive the per-msg-key is represented by PSK[Key ID], that is the pre-shared secret identified by the 'Key ID'.

4. The 128-bits long per-message encryption key is computed as:

   * per-msg-key = KDF(nonce + s + PSK[Key ID])

where the nonce is the value in the Nonce field of the Map-Request, 's' is the string "OTK-Key-Wrap", and the operation'+' just indicates string concatenation.

5. According to [RFC3394] the per-msg-key is used to wrap the OTK with AES-KEY-WRAP-128. 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.

6.5.1. Unencrypted OTK

However, when DTLS is enabled the OTK MAY be sent unencrypted as transport layer security is providing confidentiality and integrity protection.

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

6.6. Map-Resolver Processing

Upon receiving a Protected Map-Request, the Map-Resolver decapsulates the ECM message. The ITR-OTK, if encrypted, is decrypted as specified in Section 6.5.

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 6.5, 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.

6.7. Map-Server Processing

Upon receiving a Protected Map-Request, the Map-Server processes it according to the setting of the S-bit and the P-bit in the Map-Register received from the ETRs authoritative for that prefix, as described below.

While processing the Map-Request, the Map-Server can overwrite the KDF ID field if it does not support the KDF ID recommended by the ITR. Processing of the Map-Request MUST proceed in the order described in the table below, applying the processing corresponding to the first rule that matches the conditions indicated in the first column:

Matching Condition	Processing
1. At least one of the ETRs authoritative for the EID prefix included in the Map-Request registered with the P-bit set to 1	The Map-Server MUST generate a LISP-SEC protected Map-Reply as specified in Section 6.7.2. The ETR-Cant-Sign E-bit in the EID Authentication Data (EID-AD) MUST be set to 0.
2. At least one of the ETRs authoritative for the EID prefix included in the Map-Request registered with the S-bit set to 1	The Map-Server MUST generate a LISP-SEC protected Encapsulated Map-Request (as specified in Section 6.7.1), to be sent to one of the authoritative ETRs that registered with the S-bit set to 1 (and the P-bit set to 0). If there is at least one ETR that registered with the S-bit set to 0, the ETR-Cant-Sign E-bit of the EID-AD MUST be set to 1 to signal the ITR that a non LISP-SEC Map-Request might reach additional ETRs that have LISP-SEC disabled.
3. All the ETRs authoritative for the EID prefix included in the Map-Request registered with the S-bit set to 0	The Map-Server MUST send a Negative Map-Reply protected with LISP-SEC, as described in Section 6.7.2. The ETR-Cant-Sign E-bit MUST be set to 1 to signal the ITR that a non LISP-SEC Map-Request might reach additional ETRs that have LISP-SEC disabled.

Table 1: Map-Request Processing.

In this way the ITR that sent a LISP-SEC protected Map-Request always receives a LISP-SEC protected Map-Reply. However, the ETR-Cant-Sign E-bit set to 1 specifies that a non LISP-SEC Map-Request might reach additional ETRs that have LISP-SEC disabled. This mechanism allows the ITR to downgrade to non LISP-SEC requests, which does not protect against threats described in Section 4.

6.7.1. Generating a LISP-SEC Protected Encapsulated Map-Request

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 eventually received by 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-Request MUST be encapsulated in an ECM, with the S-bit set to 1, to indicate the presence of Authentication Data.

MS-OTK is wrapped with the algorithm specified by the OTK Wrapping ID field. See Section 6.5 for further details on OTK encryption. If the NULL-KEY-WRAP-128 algorithm is selected and DTLS is not enabled in the path between the Map-Server and the ETR, the Map-Request MUST be dropped and an appropriate log action SHOULD be taken.

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 MUST cover 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].

6.7.2. Generating a Proxy Map-Reply

LISP-SEC proxy Map-Reply are generated according to [I-D.ietf-lisp-rfc6833bis], with the Map-Reply S-bit set to 1. The Map-Reply includes the Authentication Data that contains the EID-AD, computed as specified in Section 6.7.1, as well as the PKT-AD computed as specified in Section 6.8.

6.8. 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 6.5 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 HMAC operation MUST cover the entire Map-Reply, where the PKT HMAC field 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].

6.9. ITR Processing: Receiving a Map-Reply

In response to a Protected Map-Request, an ITR expects a Map-Reply with the S-bit set to 1 including an EID-AD and a PKT-AD. The ITR MUST discard the Map-Reply otherwise.

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,ITR-OTK> pair associated to the Map-Reply

The integrity of the EID-AD is verified using the ITR-OTK (stored locally for the duration of this exchange) to re-compute the HMAC of the EID-AD using the algorithm specified in the EID HMAC ID field. If the ITR did indicate a Requested HMAC ID in the Map-Request and the PKT HAMC ID in the corresponding Map-Reply is different, or if the ITR did not indicate a Requested HMAC ID in the Map-Request and the PKT HMAC ID in the corresponding Map-Reply is not supported, then the ITR MUST discard the Map-Reply and send, according to rate limitation policies defined in [I-D.ietf-lisp-rfc6833bis], 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.

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 ITR did indicate a recommended KDF ID in the Map-Request and the KDF ID in the corresponding Map-Reply is different, or if the ITR did not indicate a recommended KDF ID in the Map-Request and the KDF ID in the corresponding Map-Reply is not supported, then the ITR MUST discard the Map-Reply and send, according to rate limitation policies defined in [I-D.ietf-lisp-rfc6833bis], a new Map-Request with a different KDF ID, according to ITR's local policy. The key derivation function HKDF-SHA256 MUST be supported in LISP-SEC implementations. LISP-SEC deployments SHOULD use the HKDF-SHA256 HKDF function, unless older implementations using HKDF-SHA1-128 are present in the same deployment. Without consistent configuration of involved entities, extra delays may be experienced. However, since HKDF-SHA1-128 and HKDF-SHA256 are supported, the process will eventually converge.

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 MUST discard the Map-Reply and send, according to rate limitation policies defined in [I-D.ietf-lisp-rfc6833bis], 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. When the PKT HMAC ID field does not match the Requested HMAC ID it is not possible to validate the Map-Reply.

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 6.9.1.

[I-D.ietf-lisp-rfc6833bis] allows ETRs to send Solicit-Map-Requests (SMR) directly to the ITR. The corresponding SMR-invoked Map-Request will be sent through the mapping system, hence, secured with the specifications of this memo if in use. If an ITR accepts Map-Replies piggybacked in Map-Requests and its content is not already present in its EID-to-RLOC cache, it MUST send a Map-Request over the mapping system in order to verify its content with a secured Map-Reply, before using the content.

6.9.1. 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 SHOULD be taken and the Map-Reply MUST NOT be processed any further. Implementations may include mechanisms (which are beyond the scope of this document) to avoid log resource exhaustion attacks. 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, otherwise, a log action MUST be taken and the EID-record MUST be discarded. Implementations may include mechanisms (which are beyond the scope of this document) to avoid log resource exhaustion attacks.

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

2001:db8:102::/48

2001:db8:103::/48

2001:db8:200::/40

The EID-AD contains two EID-prefixes:

2001:db8:103::/48

2001:db8:203::/48

The EID-record with EID-prefix 2001:db8:102::/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 and the EID-record MUST be discarded. Implementations may include mechanisms (which are beyond the scope of this document) to avoid log resource exhaustion attacks.

The EID-record with EID-prefix 2001:db8:103::/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:db8:200::/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 and the EID-record MUST be discarded. Implementations may include mechanisms (which are beyond the scope of this document) to avoid log resource exhaustion attacks. In this last example the ETR is trying to over claim the EID-prefix 2001:db8:200::/40, but the Map-Server authorized only 2001:db8:203::/48, hence the EID-record is discarded.

7. Security Considerations

This document extends the LISP Control-Plane defined in [I-D.ietf-lisp-rfc6833bis], hence, its Security Considerations apply as well to this document.

7.1. Mapping System Security

The LISP-SEC threat model described in Section 4, assumes that the LISP Mapping System is working properly and 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.

7.2. 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.

7.3. 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.

7.4. Deploying LISP-SEC

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 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.

7.5. Shared Keys Provisioning

Provisioning of the keys shared between ITR and Map-Resolver paris as well as between ETR and Map-Server pairs should be performed via an orchestration infrastructure and it is out of the scope of this memo. 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.

7.6. 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, in terms of resources, to a valid LISP-SEC computation and, beyond a risk of DoS attack, an attacker does not obtain any additional effect, since the corresponding Map-Reply is discarded as previously explained.

7.7. Message Privacy

DTLS [RFC9147] SHOULD be used (conforming to [RFC7525]) to provide communication privacy and to prevent eavesdropping, tampering, or message forgery to the messages exchanged between the ITR, Map-Resolver, Map-Server, and ETR, unless the OTK is encrypted in another way, e.g. using a pre-shared secret. DTLS has the responder be verified by the initiator, which enables an ITR to autheticate the Map-Resolver, and the Map-Server to authenticate the responding ETR.

7.8. 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.

8. IANA Considerations

IANA is requested to create the sub-registries listed in the following sections in the "Locator/ID Separation Protocol (LISP) Parameters" registry.

For all of the sub-registries, new values beyond this document have to be assigned according to the "Specification Required" policy defined in [RFC8126]. Expert review should assess the security properties of newly added functions, so that encryption robustness is remains strong. For instance, at the time of this writing the use of SHA-256-based functions is considered to provide sufficient protection. Consultation with security experts may be needed.

8.1. 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 6.1. Initial allocation of this registry is shown in Table 2.

Name	Number	Defined in
Reserved	0	This memo
LISP-SEC-ECM-EXT	1	This memo

Table 2: ECM Authentication Data Types.

Values 2-255 are unassigned.

8.2. 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 6.2. Initial allocation of this registry is shown in Table 3.

Name	Number	Defined in
Reserved	0	This memo
LISP-SEC-MR-EXT	1	This memo

Table 3: Map-Reply Authentication Data Types.

Values 2-255 are unassigned.

8.3. HMAC Functions

IANA is requested to create the "LISP-SEC Preferred 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. Initial allocation of this registry is shown in Table 4.

Name	Number	Defined in
NOPREF	0	This memo
AUTH-HMAC-SHA-1-96	1	[RFC2104]
AUTH-HMAC-SHA-256-128	2	[RFC6234]

Table 4: LISP-SEC Authentication Data HMAC Functions.

Values 3-65535 are unassigned.

8.4. 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. Initial allocation of this registry is shown in Table 5.

Name	Number	KEY WRAP	KDF
Reserved	0	None	None
NULL-KEY-WRAP-128	1	This memo	None
AES-KEY-WRAP-128+HKDF-SHA256	2	[RFC3394]	[RFC4868]

Table 5: LISP-SEC Authentication Data Key Wrap Functions.

Values 3-65535 are unassigned.

8.5. 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. Initial allocation of this registry is shown in Table 6.

Name	Number	Defined in
NOPREF	0	This memo
HKDF-SHA1-128	1	[RFC5869]
HKDF-SHA256	2	[RFC5869]

Table 6: LISP-SEC Authentication Data Key Derivation Function ID.

Values 2-65535 are unassigned.

9. Acknowledgements

The authors would like to acknowledge Luigi Iannone, 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.

10. References

10.1. Normative References

[I-D.ietf-lisp-rfc6830bis]
lispers.net, vaf.net Internet Consulting, 1-4-5.net, Cisco Systems, and UPC/BarcelonaTech, "The Locator/ID Separation Protocol (LISP)", draft-ietf-lisp-rfc6830bis-38 (work in progress), May 2022.

[I-D.ietf-lisp-rfc6833bis]
lispers.net, Cisco Systems, vaf.net Internet Consulting, and UPC/BarcelonaTech, "Locator/ID Separation Protocol (LISP) Control-Plane", draft-ietf-lisp-rfc6833bis-31 (work in progress), May 2022.

[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>.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, DOI 10.17487/RFC4868, May 2007, <https://www.rfc-editor.org/info/rfc4868>.

[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>.

[RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <https://www.rfc-editor.org/info/rfc7525>.

[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>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/info/rfc9147>.

10.2. Informational References

[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>.

[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>.

Authors' Addresses

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

Email: fmaino@cisco.com

Vina Ermagan
Google
California
USA

Email: ermagan@gmail.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