Internet Engineering Task Force (IETF)
Request for Comments: 9303
Category: Standards Track
ISSN: 2070-1721

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

October 2022

# Locator/ID Separation Protocol Security (LISP-SEC)

Защита протокола LISP

**Аннотация**

Этот документ описывает защиту протокола разделения идентификаторов и локаторов (Locator/ID Separation Protocol Security или LISP-SEC), представляющую собой набор механизмов аутентификации, защиты целостности и защиты от повторного использования (anti-replay) для данных отображений идентификаторов конечных точек на локаторы маршрутизации LISP (Endpoint-ID-to-Routing-Locator или EID-RLOC), передаваемых процессами поиска сопоставлений. LISP-SEC также позволяет проверять полномочность заявления префиксов EID-Prefix в сообщениях Map-Reply.

**Статус документа**

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информация о текущем статусе документа, найденных ошибках и способах обратной связи доступна по ссылке https://www.rfc-editor.org/info/rfc9303.



# Оглавление



[1]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

# 1. Введение

Протокол разделения идентификаторов и локаторов (Locator/ID Separation Protocol или LISP) [RFC9300] [RFC9301] является протоколом сетевого уровня, позволяющим разделить адреса IP на два независимых пространства - идентификаторы конечных точек (Endpoint Identifier или EID) и локаторы маршрутизации (Routing Locator или RLOC). Сопоставления EID с RLOC хранятся в базе данных и системе отображения LISP Mapping System, будучи доступными через процесс поиска Map-Request/Map-Reply. Если эти отображения EID-RLOC, передаваемые с сообщениях Map-Reply, не имеют защиты целостности, злоумышленник может манипулировать ими и захватывать коммуникации, выдавать себя за нужный EID, создавать атаки на службы (Denial-of-Service или DoS), в том числе, распределенные (Distributed Denial-of-Service или DDoS). При передаче Map-Reply без проверки подлинности враждебный элемент LISP может перезаявить EID-Prefix и перенаправить трафик. Модель угроз LISP-SEC, описанная в разделе 4, создана на основе модели угроз LISP, заданной в [RFC7835] и включающей подробное описание атак с перезаявлением (overclaiming).

Этот документ задаёт набор механизмов безопасности LISP-SEC, обеспечивающих аутентификацию источников, защиту целостности и защиту от повторного использования (anti-replay) для данных отображений EID-RLOC в LISP, передаваемых процессами поиска сопоставлений. LISP-SEC также позволяет проверять полномочность заявления EID-Prefix в сообщениях Map-Reply, гарантируя, что отправитель Map-Reply, указывающий местоположение для данного EID-Prefix, имеет право делать это в соответствии с регистрацией EID-Prefix на Map-Server. Защита Map-Register и Map-Notify, включая право элемента LISP регистрировать EID-Prefix или заявлять о его присутствии в RLOC, выходит за рамки LISP-SEC, поскольку эти протоколы защищены механизмами, заданными в [RFC9301]. Однако LISP-SEC расширяет сообщения Map-Register, позволяя входным маршрутизаторам туннелей (Ingress Tunnel Router или ITR) работать с Map-Request без LISP-SEC. Рассмотрение вопросов безопасности приведено в разделе 7.

# 2. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

# 3. Определения терминов

***One-Time Key (OTK) - одноразовый ключ***
Эфемерный случайно сгенерированный ключ, применяемый в одном обмене Map-Request - Map-Reply.

***ITR One-Time Key (ITR-OTK) - одноразовый ключ ITR***
Одноразовый ключ, созданный ITR.

***MS One-Time Key (MS-OTK) - одноразовый ключ MS***
Одноразовый ключ, созданный сервером отображений (Map-Server).

***Authentication Data (AD) - данные аутентификации***
Метаданные, включаемые в заголовок инкапсулированного управляющего сообщения LISP (Encapsulated Control Message или ECM), как указано в [RFC9301], или в сообщение Map-Reply, для поддержки защиты конфиденциальности и целостности, а также проверки полномочности EID-Prefix.

***OTK Authentication Data (OTK-AD) - данные аутентификации OTK***
Часть данных аутентификации в ECM, относящаяся к одноразовому ключу.

***EID Authentication Data (EID-AD) - данные аутентификации EID***
Часть данных аутентификации ECM и Map-Reply, применяемая для проверки полномочности EID-Prefix.

***Packet Authentication Data (PKT-AD) - данные аутентификации пакета***
Часть данных аутентификации Map-Reply, служащая для защиты целостности сообщения Map-Reply.

Определения других терминов, включая Map-Request, Map-Reply, Ingress Tunnel Router (ITR), Egress Tunnel Router (ETR), Map-Server (MS), Map-Resolver (MR), приведены в спецификации LISP [RFC9301].

# 4. Модель угроз LISP-SEC

LISP-SEC устраняет угрозы плоскости управления, описанные в параграфах 3.7 и 3.8 [RFC7835], которые нацелены на отображений EID-RLOC, включая манипуляции с сообщениями Map-Request и Map-Reply, а также злонамеренные перезаявления ETR EID-Prefix. LISP-SEC принимает 2 основных допущения: предполагается, что (1) LISP Mapping System доставляет сообщения Map-Request предусмотренному ETR, как указано EID, и (2) невозможна организация атак на пути внутри LISP Mapping System. Защита Mapping System от атак на пути зависит от конкретной системы отображения и выходит за рамки этого документа. Хотя LISP-SEC позволяет обнаруживать атаки с перезаявлением EID-Prefix, предполагается, что Map-Server могут проверять при регистрации полномочия для EID-Prefix.

В соответствии с моделью угроз из [RFC7835], в LISP-SEC предполагается, что атаки любого типа, включая атаки в пути, могут организовываться вне границ LISP Mapping System. Атакующий в пути за пределами LISP Mapping System может, например, перехватывать сообщения Map-Request и Map-Reply, подменяя отождествления узлов LISP. Другой

тип атак в пути, называемых атаками с перезаявлением (overclaiming), может быть организован вредоносным ETR, заявляющим EID-Prefix, для которых у него нет полномочий. Это позволяет ETR перенаправить трафик.

# *5. Протокольные операции*

Целью механизмов защиты, заданных в [RFC9301], является предотвращение несанкционированной вставки данных отображения за счёт аутентификации источника и защиты целостности для сообщений Map-Register, а также использования nonce для обнаружения незапрошенных сообщений Map-Reply от злоумышленников вне пути.

LISP-SEC базируется на механизмах защиты из [RFC9301] для предотвращения угроз, описанных в разделе 4, путём использования доверительных отношений между элементами LISP [RFC9301], участвующими в обмене сообщениями Map-Request и Map-Reply. Эти отношения доверия (см. 7. Вопросы безопасности и [RFC9301]) применяются для защищённого распространения (8.4. Функции Key Wrap для каждого сообщения одноразового ключа (OTK), обеспечивающего аутентификацию источника, защиту целостности и предотвращения повторного использования данных отображения в процессе поиска сопоставлений и это обеспечивает эффективную защиту от атак с перезаявлением (overclaiming). Обработка параметров защиты в процессе обмена сообщениями Map-Request и Map-Reply описана ниже.

- Для каждого сообщения Map-Request создаётся новый ключ ITR-OTK, который сохраняется в ITR и защищённо передаётся серверу Map-Server.
- Map-Server использует ITR-OTK для расчёта хэшированного кода аутентификации сообщения (Hashed Message Authentication Code или HMAC) [RFC2104], который защищает целостность данных отображения, известных Map-Server, в случае атак с перезаявлением. Map-Server также выводит новый ключ MS-OTK, который передаётся ETR, путём применения KDF (например, [RFC5869]) к ITR-OTK.
- ETR использует MS-OTK для расчёта HMAC, который защищает целостность Map-Reply, переданного ITR.
- ITR использует сохранённый ключ ITR-OTK для проверки целостности данных отображения, предоставленных Map-Server и ETR, и отсутствия атак с перезаявлением на пути между Map-Server и ITR.

В разделе 6 дано подробное описание управляющих сообщений LISP-SEC и их обработки, а в оставшейся части этого параграфа описан поток операций протокола LISP на каждом объекте, вовлеченном в обмен Map-Request и Map-Reply.

1. ITR при необходимости передать сообщение Map-Request генерирует и сохраняет OTK (ITR-OTK). Этот ключ ITR-OTK шифруется и включается в сообщение ECM, содержащее Map-Request для Map-Resolver.
2. Map-Resolver декапсулирует ECM, расшифровывает ITR-OTK (если нужно) и пересылает через Mapping System полученное сообщение Map-Request и ITR-OTK как часть нового ECM. LISP Mapping System доставляет ECM подходящему Map-Server, указанному EID получателя в Map-Request.
3. На Map-Server настроены локальные отображения и данные политики для ETR, отвечающего за EID получателя. Используя конфигурационные сведения, Map-Server после декапсуляции ECM находит наиболее подходящий (longest-match) EID-Prefix, включающий EID, запрошенный в принятом Map-Request. Map-Server добавляет этот EID-Prefix вместе с кодом HMAC, рассчитанным с помощью ITR-OTK в новое сообщение ECM, которое содержит полученное сообщение Map-Request.
4. Map-Server выводит новый ключ MS-OTK, применяя KDF к ITR-OTK. MS-OTK включается в сообщение ECM, которое Map-Server использует для пересылки Map-Request маршрутизатору ETR.
5. Если Map-Server работает в режиме посредника (proxy), как указано в [RFC9301], ETR не привлекается к созданию Map-Reply и пп. 6 и 7 пропускаются. В этом случае Map-Server создаёт Map-Reply от имени ETR, как описано в параграфе 6.7.2. Генерация Map-Reply посредником.
6. ETR при получении инкапсулированного в ECM сообщения Map-Request от Map-Server расшифровывает MS-OTK (если нужно) и формирует Map-Reply с данными отображения EID-RLOC, как указано в [RFC9301].
7. ETR рассчитывает HMAC для Map-Reply с ключом MS-OTK для защиты целостности всего сообщения Map-Reply, а также копирует сведения о полномочности EID-Prefix, которые Map-Server включил в инкапсулированный в ECM запрос Map-Request сообщения Map-Reply. После этого ETR передаёт сообщение Map-Reply запрашивающему ITR.
8. ITR при получении Map-Reply использует сохранённый локально ключ ITR-OTK для проверки целостности сведений о полномочности EID-Prefix из Map-Reply, включённых сервером Map-Server. Затем ITR рассчитывает MS-OTK применяя ту же функцию KDF (указана в инкапсулированном в ECM сообщении Map-Reply), которую использовал Map-Server и проверяет целостность Map-Reply.

# *6. Детали управляющих сообщений LISP-SEC*

Метаданные LISP-SEC, связанные с Map-Request, передаются в сообщении ECM, содержащем Map-Request, а метаданные, связанные с Map-Reply, в самом сообщении Map-Reply.

Эта спецификация использует HMAC в различных местах, как описано ниже. Реализации LISP-SEC **должны** поддерживать функцию HMAC AUTH-HMAC-SHA-256-128 [RFC6234]. В развёртываниях LISP-SEC **следует** применять функцию AUTH-HMAC-SHA-256-128, за исключением случаев, когда реализация поддерживает лишь AUTH-HMAC-SHA-1-96 [RFC2104].

## 6.1. Расширения ECM LISP-SEC

В LISP-SEC применяются сообщения ECM, определённые в [RFC9301], с установленным (1) битом S для индикации включения в заголовок LISP данных аутентификации (Authentication Data или AD). Формат LISP-SEC ECM AD показан на рисунке 1. OTK-AD обозначает данные аутентификации одноразового ключа, а EID-AD - данные аутентификации EID.

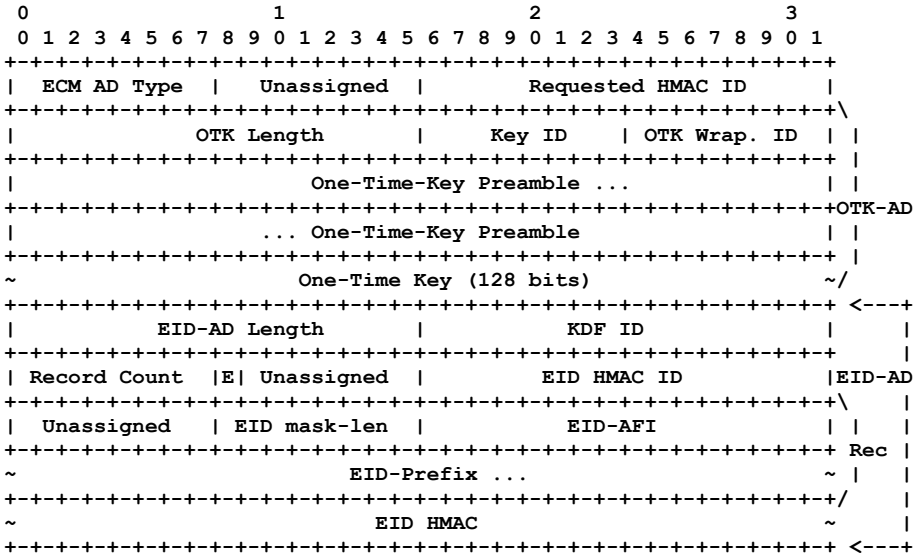


*Рисунок 1. Данные аутентификации LISP-SEC ECM.*

***ECM AD Type***
1 (LISP-SEC Authentication Data), см. раздел 8. Взаимодействие с IANA.

***Unassigned***
Устанавливается 0 при передаче и игнорируется при получении.

***Requested HMAC ID***
Алгоритм HMAC, который будет применяться для защиты отображений, запрошенных ITR. Разрешённые значения указаны в реестре LISP-SEC Authentication Data HMAC ID (параграф 8.3). Подробности даны в параграфе 6.4.

***OTK Length***
Число байтов в OTK-AD, включая OTK Preamble и OTK.

***Key ID***
Идентификатор распространённого заранее ключа, совместно используемого ITR и Map-Resolver, а также Map-Server и ETR. Такие ключи выводятся из заранее распространённого секрета для шифрования и защиты целостности OTK. Key ID позволяет менять распространённые заранее секреты без нарушения работы.

***OTK Wrapping ID (OTK Wrap. ID)***
Идентификатор функции вывода ключа (KDF) и алгоритма упаковки ключей (key wrapping), применяемых для шифрования OTK. Разрешённые значения указаны в реестре LISP-SEC Authentication Data Key Wrap ID (параграф 8.4). Подробности даны в параграфе 6.5. Шифрование и расшифровка OTK.

***One-Time-Key Preamble***
Устанавливается 0, если OTK не шифруется. При шифровании OTK это поле **может** передавать дополнительные метаданные от операции упаковки ключа. Когда 128-битовый ключ OTK передаётся без шифрования распознавателем Map-Resolver, в OTK Preamble устанавливается значение 0x0000000000000000 (64 бита). Подробности даны в параграфе 6.5.1. Нешифрованный OTK.

***One-Time-Key***
OTK, упакованный в соответствии с OTK Wrapping ID. См. параграф 6.5. Шифрование и расшифровка OTK.

***EID-AD Length***
Число байтов EID-AD. ITR **должен** указывать EID-AD Length = 4, поскольку он заполняет лишь поле KDF ID, не используя остальные части EID-AD. Данные EID-AD **могут** включать несколько EID-Record, каждая из которых занимает 4 байта плюс размер EID-Prefix с кодированием AFI.

***KDF ID***
Идентификатор функции вывода ключей (KDF), используемой для создания MS-OTK. Разрешённые значения указаны в реестре LISP-SEC Authentication Data Key Derivation Function ID (параграф 8.5). Подробности даны в параграфе 6.7. Обработка в Map-Server.

***Record Count***
В соответствии с параграфом 5.2 в [RFC9301].

***E***
Бит ETR-Cant-Sign, установка (1) которого указывает ITR, что хотя бы 1 из ETR, полномочных для EID-Prefix из этого Map-Reply, не включил LISP-SEC. Флаг может устанавливать только Map-Server (см. параграф 6.7).

***Unassigned***
Устанавливается 0 при передаче и игнорируется при получении.

***EID HMAC ID***
Идентификатор алгоритма HMAC, применяемого для защиты целостности EID-AD. Это поле устанавливает только Map-Server, рассчитывающий EID-Prefix HMAC (см. параграф 6.7.1).

***EID mask-len***
В соответствии с параграфом 5.2 в [RFC9301].

***EID-AFI***
В соответствии с параграфом 5.2 в [RFC9301].

***EID-Prefix***
В соответствии с параграфом 5.2 в [RFC9301].

***EID HMAC***
Код HMAC для EID-AD, рассчитанный и установленный Map-Server (см. параграф 6.7.1).

## 6.2. Расширения Map-Reply LISP-SEC

LISP-SEC использует сообщение Map-Reply, определённое в [RFC9301], с Type = 2 и установленным (1) битом S для индикации наличия в сообщении данных аутентификации (AD). Формат LISP-SEC Map-Reply AD показан на рисунке 2. PKT-AD - это данные аутентификации пакета, охватывающие содержимое Map-Reply.

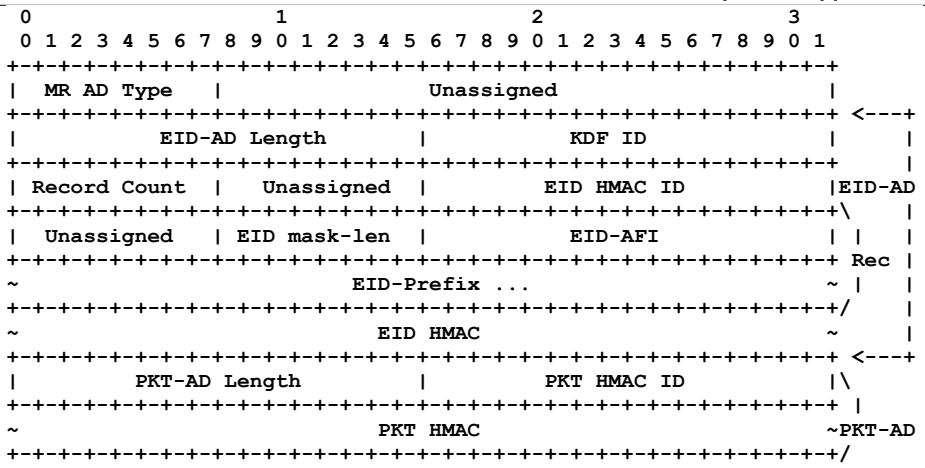


*Рисунок 2. Данные аутентификации LISP-SEC Map-Reply.*

***MR AD Type***
1 (LISP-SEC Authentication Data). См. 8. Взаимодействие с IANA.

***EID-AD Length***
Число байтов в EID-AD (см. 6.1. Расширения ECM LISP-SEC).

***KDF ID***
Идентификатор функции KDF, используемой для вывода MS-OTK (см. 6.1. Расширения ECM LISP-SEC).

***Record Count***
Число записей в сообщении Map-Reply (см. 6.1. Расширения ECM LISP-SEC).

***Unassigned***
Устанавливается 0 при передаче и игнорируется при получении.

***EID HMAC ID***
Идентификатор алгоритма HMAC, применяемого для защиты целостности EID-AD (см. 6.1. Расширения ECM LISP-SEC).

***EID mask-len***
Размер маски для EID-Prefix (см. 6.1. Расширения ECM LISP-SEC).

***EID-AFI***
См. 6.1. Расширения ECM LISP-SEC.

***EID-Prefix***
См. 6.1. Расширения ECM LISP-SEC.

***EID HMAC***
См. 6.1. Расширения ECM LISP-SEC.

***PKT-AD Length***
Число байтов в PKT-AD.

***PKT HMAC ID***
Идентификатор алгоритма HMAC, применяемого для защиты целостности Map-Reply (см. 6.5. Шифрование и расшифровка OTK).

***PKT HMAC***
Код HMAC всего пакета Map-Reply для защиты его целостности, включая данные LISP-SEC AD (из поля Map-Reply Type в поле PKT HMAC), позволяющие аутентифицировать сообщение.

## 6.3. Расширения Map-Register LISP-SEC

Бит S в сообщении Map-Register (см. [RFC9301]) указывает серверу Map-Server, что регистрируемый ETR поддерживает LISP-SEC. ETR с поддержкой LISP-SEC **должен** устанавливать (1) флаг S в сообщениях Map-Register.

## 6.4. Обработка в ITR - генерация Map-Request

При создании Map-Request маршрутизатор ITR генерирует случайный ключ ITR-OTK, сохраняя его локально до получения соответствующего Map-Reply (6.9. Обработка в ITR - приём Map-Reply) вместе с nonce, создаваемым как указано в [RFC9301].

ITR **может** использовать поле KDF ID для указания рекомендуемого алгоритма KDF в соответствии с локальными правилами. Map-Server может переопределить KDF ID, если он не поддерживает рекомендованный ITR алгоритм (6.7. Обработка в Map-Server). Значение KDF NOPREF (0) может служить для указания отсутствия у ITR предпочтительного KDF ID.

Для пути между ITR и Map-Resolver **должна** обеспечиваться защита конфиденциальности и целостности с помощью ITR-OTK. Это можно реализовать путём шифрования ITR-OTK с использованием заранее распространённого секрета для ITR и Map-Resolver (6.5. Шифрование и расшифровка OTK) или включения DTLS [RFC9147] между ними.

Сообщения Map-Request (как задано в [RFC9301]) **должны** инкапсулироваться как управляющие сообщения LISP в ECM с установленным (1) флагом S для индикации наличия данных аутентификации (AD). Такие сообщения в этом документе называются дакже защищёнными (Protected) Map-Request.

ITR-OTK упаковывается с использованием алгоритма, указанного полем OTK Wrapping ID (шифрование OTK описано в параграфе 6.5). При выборе алгоритма NULL-KEY-WRAP-128 (8.4. Функции Key Wrap) и отсутствии иного механизма шифрования (например, DTLS) на пути между ITR и Map-Resolver, сообщение Map-Request **должно** отбрасываться, а в системном журнале **следует** оставлять соответствующую запись. Реализации могут включать механизмы предотвращения атак на истощение ресурсов системного журнала, но это выходит за рамки документа.

Поле Requested HMAC ID указывает алгоритм HMAC, предложенный для использования Map-Server и ETR с целью защиты целостности ECM AD и Map-Reply. HMAC ID со значением NONE (0) **можно** использовать, если у ITR нет пердпочтений для HMAC ID.

Поле KDF ID указывает функцию KDF, предложенную для использования на Map-Server при выводе MS-OTK. **Можно** указать KDF с идентификатором NONE (0), если у ITR нет предпочтений для KDF ID.

В поле EID-AD Length указывается значение 4, поскольку данные аутентификации (AD) не включают EID-Prefix AD и EID-AD содержит лишь поле KDF ID.

Если ITR напрямую соединён с Mapping System, такой как LISP+ALT [RFC6836], он выполняет функции ITR и Map-Resolver, пересылая защищённые Map-Request, как указано в 6.6. Обработка в Map-Resolver.

Обработка на Proxy ITR (PITRs) эквивалентна обработке на ITR, поэтому применяются описанные выше процедуры.

## 6.5. Шифрование и расшифровка OTK

Защита конфиденциальности и целостности MS-OTK должна обеспечиваться на пути между Map-Server и ETR. Это можно реализовать за счёт применения DTLS между Map-Server и ETR или шифрования MS-OTK с заранее распространенным секретом, известным Map-Server и ETR [RFC9301]. Точно так же **должна** обеспечиваться конфиденциальность и целостность ITR-OTK на пути между ITR и Map-Resolver, которая может быть достигнута такими же способами. Общий ключ ITR и Map-Resolver подобен общему ключу Map-Server и ETR.

В этом параграфе описана обработка OTK на пути ITR - Map-Resolver и Map-Server - ETR.

Важно отметить, что для предотвращения атак с перезаявлением от ETR общий ключ ITR и Map-Resolver **должен** быть независимым от общего ключа Map-Server и ETR.

OTK упаковывается с помощью алгоритма, указанного полем OTK Wrapping ID, которое задает:

- алгоритм Key Encryption Algorithm, применяемый для шифрования упаковываемого OTK;
- функцию вывода ключей KDF для создания ключа шифрования для каждого сообщения.

Реализации этой спецификации **должны** поддерживать OTK Wrapping ID AES-KEY-WRAP-128+HKDF-SHA256, задающий применение функции вывода ключей HKDF-SHA256, заданной в [RFC5869], для создания ключей шифрования каждого сообщения (per-msg-key), а также алгоритм упаковки ключей AES-KEY-WRAP-128 для шифрования 128-битовых OTK, в соответствии с [RFC3394].

Реализации этой спецификации **должны** поддерживать OTK Wrapping NULL- KEY-WRAP-128, применяемый для передачи нешифрованных 128-битовых OTK с преамбулой 0x0000000000000000 (64 бита).

Процесс упаковки для OTK Wrapping ID AES-KEY-WRAP-128+HKDF- SHA256 описан ниже.

1. KDF и алгоритмы упаковки ключей указываются значением поля OTK Wrapping ID. Начальные значения идентификаторов указаны в таблице 5.
2. Если выбран алгоритм NULL-KEY-WRAP-128 (8.4. Функции Key Wrap) и протокол DTLS не включён, сообщение Map-Request **должно** отбрасываться а в системный журнал **следует** вносить соответствующую запись. Разработчики могут реализовать механизмы защиты от истощения ресурсов системного журнала, но это выходит за рамки данного документа.
3. Заранее распространённый секрет, применяемый для вывода per-msg-key, представляется PSK[Key ID], указывающим распределенный заранее секрет, указанный индексом Key ID.
4. 128-битовый ключ шифрования рассчитывается, как показано ниже

   ```
   per-msg-key = KDF( nonce + s + PSK[Key ID] )
   ```
   где nonce - значение поля Nonce из Map-Request, s - строка OTK-Key-Wrap, а + указывает конкатенацию.
5. Ключ per-msg-key применяется для упаковки OTK с помощью AES-KEY-WRAP-128, как указано в параграфе 2.2.1 [RFC3394]. Для инициализации упаковки ключа AES (Key Wrap Initialization) **должно** использоваться значение 0xA6A6A6A6A6A6A6A6 (64 бита). Результатом упаковки ключа AES является 192-битовое значение, старшие 64 бита которого копируются в поле One-Time Key Preamble, а оставшиеся 128 младших битов - в поле One-Time Key данных аутентификации LISP-SEC AD.

При расшифровке ключа OTK получатель **должен** убедиться, что значение Initialization Value, полученное при расшифровке упакованного ключа AES, равно 0xA6A6A6A6A6A6A6A6. Если это не так, получатель **должен** отбросить сообщение целиком.

### *6.5.1. Нешифрованный OTK*

При включённом протоколе DTLS ключ OTK **можно** передавать без шифрования, поскольку защита транспортного уровня обеспечивает целостность и конфиденциальность.

При передаче 128-битового OTK без шифрования для OTK Wrapping ID устанавливается значение NULL_KEY_WRAP_128, а для OTK Preamble - 0x0000000000000000 (64 бита).

## 6.6. Обработка в Map-Resolver

При получении защищённого Map-Request распознаватель Map-Resolver декапсулирует ECM, расшифровывая ITR-OTK (если это нужно) в соответствии с параграфом 6.5. Шифрование и расшифровка OTK.

Защита конфиденциальности ITR-OTK и безопасность в целом после того, как Map-Request передаётся распознавателем Map-Resolver на Map-Server, зависит от применяемой Mapping System и выходит за рамки документа.

В системах отображения, где Map-Server соответствует [RFC9301], Map-Resolver создаёт новый заголовок ECM с установленным (1) битом S, который содержит нешифрованный ключ ITR-OTK, как указано в параграфе 6.5, и другие данные, полученные из ECM Authentication Data принятого инкапсулированного сообщения Map-Request.

Затем Map-Resolver пересылает серверу Map-Server полученное сообщение Map-Request, которое инкапсулируется с новым заголовком ECM, включающим недавно рассчитанные поля Authentication Data.

## 6.7. Обработка в Map-Server

При получении защищённого Map-Request сервер Map-Server обрабатывает его в соответствии с установкой битов S и P в Map-Register от полномочных для префикса ETR, как описано ниже.

При обработке Map-Request сервер Map-Server может переопределить поле KDF ID, если он не поддерживает функцию KDF, рекомендованную ITR. Обработка Map-Request **должна** выполняться в порядке, указанном в таблице 1, путём выполнения первого правила, соответствующего условиям, указанным в первом столбце.

*Таблица 1. Обработка Map-Request.*

| ***Условия совпадения*** | ***Обработка*** |
|---|---|
| 1. Хотя бы 1 ETR полномочен для EID-Prefix, включённого в Map-Request, зарегистрированный с битом P=1. | Map-Server **должен** генерировать защищённое LISP-SEC сообщение Map-Reply, как указано в параграфе 6.7.2. Бит ETR-Cant-Sign (E) в EID-AD должен быть сброшен (0). |
| 2. Хотя бы 1 ETR полномочен для EID-Prefix, включённого в Map-Request, зарегистрированный с битом S=1. | Map-Server **должен** генерировать защищённое LISP-SEC инкапсулипрванное сообщение Map-Request (параграф 6.7.1) для передачи одному из полномочных ETR, зарегистрированных с установленным (1) битом S (и битом P=0). Если имеется хотя бы 1 ETR, зарегистрированный с S=0, флаг ETR-Cant-Sign (E) в EID-AD **должен** быть установлен (1) для указания ITR, что Map-Request без LISP-SEC может достичь ETR с отключённым LISP-SEC. |
| 3. Все ETR полномочны для EID-Prefix, включённого в Map-Request, зарегистрированный с битом S=0. | Map-Server **должен** передать сообщение Negative Map-Reply, защищенное LISP-SEC, как описано в параграфе 6.7.2. Флаг ETR-Cant-Sign (E) должен быть установлен (1) для указания ITR, что Map-Request без LISP-SEC может достичь ETR с отключённым LISP-SEC. |

Таким образом, ITR передающий Map-Request с защитой LISP-SEC всегда получает защищённые LISP-SEC отклики Map-Reply. Однако установленный (1) флаг ETR-Cant-Sign (E) указывает, что Map-Request без защиты LISP-SEC может достичь ETR, на которых нет LISP-SEC. Этот механизм позволяет ITR обрабатывать запросы без LISP-SEC, которые не защищены от угроз, указанных в разделе 4.

### *6.7.1. Генерация защищённых LISP-SEC сообщений Map-Request*

Map-Server декапсулирует ECM и генерирует новые данные аутентификации ECM AD, включающие OTK-AD и EID-AD с сведениями о полномочиях EID-Prefix, которые в конечном итоге получены запрашивающим ITR. Map-Server обновляет OTK-AD, выводя новый ключ OTK (MS-OTK) из ITR-OTK, полученного с Map-Request. MS-OTK выводится с применением функции KDF, заданной полем KDF ID. Если указанный KDF ID алгоритм не поддерживается, Map-Server использует другой алгоритм с соответственно обновляет поле KDF ID. Сообщение Map-Request **должно** инкапсулироваться в ECM с установленным (1) битом S для индикации наличия данных аутентификации (AD).

MS-OTK упаковывается с помощью алгоритма, заданного полем OTK Wrapping ID (см. 6.5. Шифрование и расшифровка OTK). При использовании алгоритма NULL-KEY-WRAP-128 и отсутствии DTLS на пути между Map-Server и ETR сообщение Map-Request **должно** отбрасываться и это **следует** записывать в системный журнал.

Map-Server включает в EID-AD самый длинный из совпадающих зарегистрированных EID-Prefix для EID получателя и код HMAC для этого EID-Prefix. HMAC рассчитывается с ключом ITR-OTK из полученных ECM AD с применением алгоритма, выбранного в соответствии с полем Requested HMAC ID. Если Map-Server не поддерживает этот алгоритм, но применяет свой и указывает его в поле EID HMAC ID. При расчёте HMAC **должны** использоваться данные EID-AD целиком, от поля EID-AD Length до EID HMAC, которое для расчёта **должно** устанавливаться в 0.

Затем Map-Server пересылает инкапсулированное в ECM обновлённое сообщение Map-Request, содержащее OTK-AD, EID-AD и полученное сообщение Map-Request, полномочному ETR, как указано в [RFC9301].

### *6.7.2. Генерация Map-Reply посредником*

Защищённое LISP-SEC сообщение Map-Reply от посредника генерируется в соответствии с [RFC9301] и имеет установленный (1) бит S. Map-Reply включает данные аутентификации AD с данными EID-AD, рассчитанными в соответствии с параграфом 6.7.1, а также данными PKT-AD, рассчитанными с соответствии с параграфом 6.8.

## 6.8. Обработка в ETR

При получении инкапсулированного в ECM сообщения Map-Request с установленным (1) битом S маршрутизатор ETR декапсулирует ECM. Поле OTK расшифровывается (если оно зашифровано) в соответствии с параграфом 6.5 для получения нешифрованного ключа MS-OTK. Затем ETR генерирует Map-Reply, как указано в [RFC9301] и включает в него данные аутентификации AD с EID-AD из принятого инкапсулированного Map-Request, а также PKT-AD.

Данные EID-AD копируются из Authentication Data в принятом инкапсулированном сообщении Map-Request. PKT-AD содержит код HMAC для всего пакета Map-Reply, созданный с ключом MS-OTK и алгоритмом HMAC, заданным в поле Requested HMAC ID полученного инкапсулированного Map-Request. Если ETR не поддерживает запрошенный алгоритм HMAC, он использует иной алгоритм, указывая его в поле PKT HMAC ID. Операция HMAC **должна** охватывать Map-Reply целиком, а для поля PKT HMAC при расчёте **должно** устанавливаться значение 0.

ETR передаёт сообщение Map-Reply запрашивающему ITR, как указано в [RFC9301].

## 6.9. Обработка в ITR - приём Map-Reply

В ответ на защищённое сообщение Map-Request маршрутизатор ITR ожидает получить Map-Reply с установленным (1) битом S, включающее EID-AD и PKT-AD. В противном случае ITR **должен** отбросить Map-Reply.

При получении Map-Reply маршрутизатор ITR должен проверить целостность EID-AD и PKT-AD, а при обнаружении нарушения **должен** отбросить Map-Reply. После обработки Map-Reply маршрутизатор ITR **должен** отбросить пару <nonce, ITR-OTK>, счязанную с Map-Reply.

Целостность EID-AD проверяется с применением ITR-OTK (сохранен локально на время этого обмена) для перерасчёта HMAC данных EID-AD с использованием алгоритма, заданного в поле EID HMAC ID. Если ITR указал Requested HMAC ID в своём сообщении Map-Request, а PKT HAMC ID в соответствующем Map-Reply отличается или ITR не указывал Requested HMAC ID в Map-Request, при этом PKT HMAC ID в соответствующем Map-Reply не поддерживается ITR, тот **должен** отбросить Map-Reply и передать (с учётом правил ограничения частоты из [RFC9301]) новое сообщение Map-Request с другим значением Requested HMAC ID в соответствии с локальной политикой ITR. Код HMAC вычисляется для всех данных EID-AD, начиная от EID-AD Length и заканчивая EID HMAC, при расчёте HMAC маршрутизатор ITR **должен** установить в поле EID HMAC значение 0.

Для проверки целостности PKT-AD сначала выводится MS-OTK из сохранённого локально ITR-OTK с применением алгоритма, заданного полем KDF ID. Это обусловлено тем, что при создании PKT-AD в ETR использовался ключ MS-OTK. Если ITR указал рекомендуемый KDF ID в своём Map-Request, а KDF ID из соответствующего Map-Reply отличается или ITR не указывал рекомендуемого KDF ID в своём Map-Request, тот **должен** отбросить Map-Reply и передать (с учётом правил ограничения частоты из [RFC9301]) новое сообщение Map-Request с другим значением KDF ID в соответствии с локальной политикой ITR. Реализации LISP-SEC **должны** поддерживать функцию KDF HKDF-SHA256, а развёртываниям LISP-SEC **следует** применять её, если в том же развёртывании нет более старой реализации, использующей HKDF-SHA1-128. Без согласования настройки вовлечённых элементов могут возникать дополнительные задержки, однако процесс сходится со временем, благодаря поддержке HKDF-SHA1-128 и HKDF-SHA256.

Затем выведенное значение MS-OTK применяется для пересчёта HMAC из PKT-AD с применением алгоритма, указанного в поле PKT HMAC ID. Если поле PKT HMAC ID не совпадает с Requested HMAC ID, ITR **должен** отбросить Map-Reply и передавать (с учётом правил ограничения частоты из [RFC9301]) новое сообщение Map-Request с другим значением Requested HMAC ID в соответствии с локальной политикой, пока не переберёт все поддерживаемые ITR значения HMAC ID. Несовпадение значений PKT HMAC ID и Requested HMAC ID не позволяет проверить Map-Reply.

Отдельная запись EID-Record в Map-Reply считается действительной, если (1) оба поля EID-AD и PKT-AD действительны и (2) непусто пересечение EID-Prefix в EID-Record из Map-Reply с одним из EID-Prefix из EID-AD. После идентификации действительности записи Map-Reply маршрутизатор ITR устанавливает для EID-Prefix в записи Map-Reply значение набора пересечений, рассчитанных ранее и добавляет EID-Record из Map-Reply в свой кэш EID-RLOC Map-Cache, как описано в [RFC9301]. Пример проверки записи Map-Reply представлен в параграфе 6.9.1.

[RFC9301] разрешает ETR передавать сообщения SMR (Solicit-Map-Request) напрямую ITR. Вызванное таким SMR сообщение Map-Request будет передаваться через Mapping System и поэтому будет защищено в соответствии с этой спецификацией, если она применяется. Если ITR воспринимает Map-Reply, прицепленные к Map-Request, и их содержимого ещё нет в его EID-RLOC Map-Cache, маршрутизатор **должен** передать Map-Request через Mapping System, чтобы проверить содержимое с помощью защищённого Map-Reply до использования.

### *6.9.1. Проверка записей в Map-Reply*

Содержимое Map-Reply может включать записи EID-Record. Сообщение Map-Reply целиком подписано ETR с кодом HMAC PKT для защиты целостности и аутентификации источника EID-Prefix, заявляемых ETR. Поле Authentication Data в Map-Reply может включать несколько EID-Records в EID-AD. Данные EID-AD подписывает Map-Server кодом HMAC EID для защиты целостности и аутентификации источника EID-Prefix, вставленных Map-Server.

При получении Map-Reply с установленным (1) флагом S маршрутизатор ITR сначала проверяет коды HMAC для EID и PKT-AD. Несоответствии любого из HMAC **следует** записать в системный журнал, а Map-Reply **недопустимо** обрабатывать дальше. Реализации могут включать механизмы предотвращения атак с истощением ресурсов ведения журнала (это выходит за рамки документа). Если оба кода HMAC действительны, ITR выполняет проверку каждой EID-Record, заявленной ETR, путём расчёта пересечения каждого включённого EID-Prefix из Map-Reply с каждым из EID-Prefix в EID-AD. Запись EID-Record действительная лишь при непустом пересечении, в противном случае **должна** вноситься запись в системный журнал, а запись EID-Record **должна** отбрасываться. Реализации могут включать механизмы предотвращения атак с истощением ресурсов ведения журнала (выходит за рамки документа).

Например, для Map-Reply с тремя записями отображений EID-Prefix

```
2001:db8:102::/48
2001:db8:103::/48
2001:db8:200::/40
```

EID-AD будет содержать 2 EID-Prefix

```
2001:db8:103::/48
2001:db8:203::/48
```

EID-Record с EID-Prefix 2001:db8:102::/48 не выбрана для использования ITR, поскольку она не включена ни в одну из EID-AD, подписанных Map-Server. В системный журнал **должна** помещаться запись об этом, а EID-Record **должна** быть отброшена. Реализации могут включать механизмы предотвращения атак с истощением ресурсов ведения журнала (выходит за рамки документа).

EID-Record с EID-Prefix 2001:db8:103::/48 выбрана для использования ITR, поскольку она соответствует второму EID-Prefix из EID-AD.

EID-Record с EID-Prefix 2001:db8:200::/40 не выбрана для использования ITR, поскольку она не включена ни в одну из EID-AD, подписанных Map-Server. В системный журнал **должна** помещаться запись об этом, а EID-Record **должна** быть отброшена. Реализации могут включать механизмы предотвращения атак с истощением ресурсов ведения журнала

(выходит за рамки документа). В этом последнем случае ETR пытается перезаявить EID-Prefix 2001:db8:200::/40, но Map-Server разрешил только 2001:db8:203::/48; поэтому EID-Record отбрасывается.

# *7. Вопросы безопасности*

Этот документ расширяет плоскость управления LISP, заданную в [RFC9301], поэтому соображения безопасности из этого документа применимы и здесь.

## 7.1. Безопасность системы отображения

Модель угроз LISP-SEC, описанная в разделе 4, предполагает, что система отображения LISP работает корректно и доставляет сообщения Map-Request серверу Map-Server, который полномочен для запрошенного EID.

Предполагается, что Mapping System обеспечивает конфиденциальность OTK и целостность данных Map-Reply. Однако способы защиты LISP Mapping System выходят за рамки этого документа.

Безопасность Map-Register, включая права элементов LISP регистрировать EID-Prefix или заявлять наличие RLOC также выходит за рамки LISP-SEC.

## 7.2. Генерация случайных значений

Ключи ITR-OTK **должны** генерироваться источником псевдослучайных (или строго случайных) значений с подобающей затравкой (seed). Рекомендации по созданию случайных значений представлены в [RFC4086].

## 7.3. Совмещение Map-Server и ETR

Если Map-Server совмещён с ETR, LISP-SEC не обеспечивает защиты от атак с перезаявлением со стороны этого ETR. Однако в этом конкретном случае, где ETR размещается в доверенной области Map-Server, атаки с перезаявлением от ETR не включены в модель угроз.

## 7.4. Внедрение LISP-SEC

При внедрении LISP-SEC в соответствии с этим документом следует тщательно взвесить применимость модели угроз LISP-SEC к данному варианту развёртывания и применения. Если принимается решение об игнорировании тех или иных рекомендаций, следует учитывать связанный с этим риск.

Например, в некоторых других развёртываниях злоумышленники могут оказаться очень изощрёнными и это вынудит применять при внедрении очень строгие правила в части алгоритмов HMAC, воспринимаемых ITR.

Аналогичные соображения применимы ко всей модели угроз LISP-SEC, поэтому при разработке и внедрении следует внимательно относиться к рекомендациям, которые указаны в этом документе уровнем **следует**.

## 7.5. Предоставление общих ключей

Предоставление ключей, совместно используемых парой ITR и Map-Resolver или ETR и Map-Server следует организовывать через инфраструктуру оркестровки, которая выходит за рамки этого документа. Рекомендуется периодически обновлять оба этих ключа, чтобы они не устаревали и злоумышленники не получали к ним несанкционированного доступа. Для общих ключей следует использовать непредсказуемые случайные значения.

## 7.6. Replay-атаки

Злоумышленники могут захватывать действительные сообщения Map-Request или Map-Reply и повторно использовать их (replay). Однако, как только ITR получает исходное сообщение Map-Reply, пара <nonce,ITR-OTK>, хранящаяся в ITR, отбрасывается. При получении воспроизводимого сообщения Map-Reply маршрутизатором ITR у него не будет пары <nonce,ITR-OTK>, соответствующей полученному Map-Reply и это сообщение будет отброшено.

При повторном использовании Map-Request элементы Map-Server, Map-Resolver и ETR должны выполнять расчёт LISP-SEC. С точки зрения ресурсов это эквивалентного легитимным расчётам LISP-SEC, поэтому кроме возможности организации DoS-атаки, злоумышленник не получает дополнительного эффекта, поскольку сообщение отбрасывается, как отмечено выше.

## 7.7. Приватность сообщений

**Следует** использовать DTLS [RFC9147] (в соответствии с [RFC7525]) для защиты приватности взаимодействий и предотвращения перехвата, изменения и подделки сообщений, передаваемых между ITR, Map-Resolver, Map-Server, ETR, если ключи OTK не шифруются иными средствами, например с использованием заранее распространённого секрета. Ответчик DTLS проверяет инициатора, что позволяет ITR проверить подлинность Map-Resolver, Map-Server - подлинность отвечающего ETR.

## 7.8. DoS и DDoS-атаки

LISP-SEC снижает риск атак DoS и DDoS, защищая целостность сообщений и проверяя подлинность источников Map-Request и Map-Reply, а также предотвращая перезаявление EID-Prefix вредоносными ETR, которое могло бы перенаправить трафик на большое число хостов.

# *8. Взаимодействие с IANA*

Агентство IANA создало указанные в последующих параграфах субреестры в реестре Locator/ID Separation Protocol (LISP) Parameters. Во всех этих субреестрах новые значения выделяются по процедуре Specification Required, заданной в [RFC8126]. В рецензии экспертов (Expert Review) следует оценивать защитные свойства добавляемых функций, чтобы сохранялось строгое шифрования. Например, на момент создания этого документа применение функций на основе SHA-256 считалось достаточным для защиты. Могут потребоваться консультации со специалистами по безопасности.

## 8.1. Реестр типов ECM AD

Агентство IANA создало реестр LISP ECM Authentication Data Types со значениями от 0 до 255 для использования в расширениях LISP-SEC ECM (6.1. Расширения ECM LISP-SEC). Исходное содержимое реестра приведено в таблице 2.

*Таблица 2. Типы LISP ECM Authentication Data.*

| Имя | Номер | Документ |
|---|---|---|
| Резерв | 0 | RFC 9303 |
| LISP-SEC-ECM-EXT | 1 | RFC 9303 |

Значения 2 - 255 не выделены.

## 8.2. Реестр типов Map-Reply AD

Агентство IANA создало реестр LISP Map-Reply Authentication Data Types со значениями от 0 до 255 для использования в расширениях LISP-SEC Map-Reply (6.2. Расширения Map-Reply LISP-SEC). Исходное содержимое реестра приведено в таблице 3.

*Таблица 3. Типы Map-Reply Authentication Data.*

| Имя | Номер | Документ |
|---|---|---|
| Резерв | 0 | RFC 9303 |
| LISP-SEC-MR-EXT | 1 | RFC 9303 |

Значения 2 - 255 не выделены.

## 8.3. Функции HMAC

Агентство IANA создало реестр LISP-SEC Preferred Authentication Data HMAC IDs со значениями от 0 до 65535 для использования в качестве Requested HMAC ID, EID HMAC ID, PKT HMAC ID в данных аутентификации LISP-SEC AD. Исходное содержимое реестра приведено в таблице 4.

*Таблица 4. Идентификаторы LISP-SEC Preferred Authentication Data HMAC.*

| Имя | Номер | Документ |
|---|---|---|
| NOPREF | 0 | RFC 9303 |
| AUTH-HMAC-SHA-1-96 | 1 | [RFC2104] |
| AUTH-HMAC-SHA-256-128 | 2 | [RFC6234] |

Значения 3 - 65535 не выделены.

## 8.4. Функции Key Wrap

Агентство IANA создало реестр LISP-SEC Authentication Data Key Wrap IDs со значениями от 0 до 65535 для использования в качестве идентификаторов алгоритма упаковки ключей OTK в LISP-SEC AD. Исходное содержимое реестра приведено в таблице 5.

*Таблица 5. Идентификаторы LISP-SEC Authentication Data Key Wrap.*

| Имя | Номер | Key Wrap | KDF | Документ |
|---|---|---|---|---|
| Резерв | 0 | Нет | Нет | RFC 9303 |
| NULL-KEY-WRAP-128 | 1 | RFC 9303 | None | RFC 9303 |
| AES-KEY-WRAP-128+HKDF-SHA256 | 2 | [RFC3394] | [RFC4868] | RFC 9303 |

Значения 3 - 65535 не выделены.

## 8.5. Функции вывода ключей

Агентство IANA создало реестр LISP-SEC Authentication Data Key Derivation Function IDs со значениями от 0 до 65535 для использования в качестве KDF ID. Исходное содержимое реестра приведено в таблице 6.

*Таблица 6. Идентификаторы LISP-SEC Authentication Data Key Derivation Function.*

| Имя | Номер | Документ |
|---|---|---|
| NOPREF | 0 | RFC 9303 |
| HKDF-SHA1-128 | 1 | [RFC5869] |
| HKDF-SHA256 | 2 | [RFC5869] |

Значения 3 - 65535 не выделены.

# *9. Литература*

## 9.1. Нормативные документы

[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>.

[RFC9300] Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A. Cabellos, Ed., "The Locator/ID Separation Protocol (LISP)", RFC 9300, DOI 10.17487/RFC9300, October 2022, <https://www.rfc-editor.org/info/rfc9300>.

[RFC9301] Farinacci, D., Maino, F., Fuller, V., and A. Cabellos, Ed., "Locator/ID Separation Protocol (LISP) Control Plane", RFC 9301, DOI 10.17487/RFC9301, October 2022, <https://www.rfc-editor.org/info/rfc9301>.

## 9.2. Дополнительная литература

[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>.

## *Благодарности*

Авторы благодарны Luigi Iannone, Pere Monclus, Dave Meyer, Dino Farinacci, Brian Weis, David McGrew, Darrel Lewis, Landon Curt Noll за их полезные предложения в процессе подготовки этого документа.

## *Адреса авторов*

**Fabio Maino**
Cisco Systems
San Jose, CA
United States of America
Email: fmaino@cisco.com

**Vina Ermagan**
Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
United States of America
Email: ermagan@gmail.com

**Albert Cabellos**
Universitat Politecnica de Catalunya
c/ Jordi Girona s/n
08034 Barcelona
Spain
Email: acabello@ac.upc.edu

**Damien Saucez**
Inria
2004 route des Lucioles - BP 93
Sophia Antipolis
France
Email: damien.saucez@inria.fr

**Перевод на русский язык**

Николай Малых

nmalykh@protokols.ru