Internet Engineering Task Force (IETF)
Request for Comments: 8003
Obsoletes: 5203
Category: Standards Track
ISSN: 2070-1721

J. Laganier
Luminate Wireless, Inc.
L. Eggert
NetApp

October 2016

Host Identity Protocol (HIP) Registration Extension

Регистрационное расширение протокола HIP

Аннотация

Этот документ задаёт механизм регистрации для протокола идентификации хостов (Host Identity Protocol или HIP), который позволяет хостам регистрироваться в таких службах, как серверы встречи HIP (rendezvous) и промежуточные устройства. Документ отменяет действие RFC 5203.

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.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc8003.

Оглавление

1. Введение

Этот документ содержит расширение для протокола идентификации хостов (Host Identity Protocol или HIP) [RFC7401]. Расширение обеспечивает хостам базовые способы регистрации в службах, которыми могут служить, например, серверы «встречи» HIP (rendezvous) [RFC8004] или промежуточные устройства [RFC3234].

Документ не содержит допущений о конкретных типах сервиса, а также не задаёт каких-либо механизмов обнаружения конкретных служб или способов взаимодействия с ними после регистрации. Эти операции могут быть описаны в будущих документах.

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

Ключевые слова **должно** (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 [RFC2119].

2. Термины

В дополнение к терминам, определенным в документе HIP Architecture [HIP-ARCH], спецификации HIP [RFC7401] и Rendezvous Extension [RFC8004], этот документ добавляет ещё несколько приведённых ниже определений.

Requester - заявитель (регистрируемый)
Узел HIP, обращающийся в регистратору HIP для запроса регистрации в службе.

Registrar - регистратор
Узел HIP, предлагающий регистрацию в одной или нескольких службах.

Service - служба
Возможность (функция), предоставляющая заявителям новые функции, работающие на уровне HIP. Примеры включают межсетевые экраны с поддержкой HIP, серверы встречи HIP.

Registration - регистрация
Общее состояние, сохраняемое заявителем и регистратором и позволяющее заявителю использовать одну или несколько служб, предлагаемых регистратором. Для каждой регистрации задаётся конечный срок действия. Заявители могут продлять регистрацию повторением процедуры (обновлением).

Registration Type - тип регистрации
8-битовый идентификатор для данной службы в протоколе регистрации. Например, сервис rendezvous указывается конкретным типом регистрации.

3. Обзор регистрационного расширения HIP

Документ не задаёт способов обнаружения заявителями доступности сервиса или нахождения регистратора. После обнаружения регистратора заявителем тот инициирует базовый обмен HIP или использует имеющуюся ассоциацию с регистратором. В обоих случаях регистраторы используют дополнительные параметры, определённые в этом документе (см. ниже), для анонсирования себя и предоставления или отклонения регистрации. Заявители используют соответствующие параметры для регистрации в службе. Обе стороны **могут** также включать в обмен сообщениями дополнительные параметры HIP, связанные с запрашиваемым типом регистрации. Такие параметры и способы их применения будут заданы в других документах.

Базовый обмен HIP, включая определения пакетов HIP I1, R1, I2, R2, определён в [RFC7401]. В последующих параграфах описаны различия между регистрационным согласованием и обычным базовым обменом HIP [RFC7401].

3.1. Анонсирование возможностей регистратором

Хосту, способному и желающему служить регистратором для конкретного хоста, **следует** включить параметр REG_INFO в пакеты R1, передаваемый в базовом обмене с этим заявителем. Если хост временно не способен предоставить услугу, ему **следует** передать пустой параметр REG_INFO (без указания услуг). Если позднее услуги могут быть предоставлены, **следует** передать пакеты UPDATE, указывающие текущий набор доступных услуг в новом параметре REG_INFO, всем хостам, с которыми данный хост связан.

3.2. Запрос регистрации заявителем

Для запроса регистрации в службе заявитель создаёт соответствующий параметр REG_REQUEST и включает его в пакет I2 или UPDATE, передаваемый регистратору.

Если у заявителя ещё нет ассоциации HIP с регистратором, ему **следует** передать параметр REG_REQUEST как можно раньше, т. е. в пакете I2. Это минимизирует число пакетов, которыми нужно обменяться с регистратором. Регистратор **может** завершить ассоциацию HIP, в которой не передан параметр REG_REQUEST, включив NOTIFY типа REG_REQUIRED в пакет R2. В этом случае между хостами не будет создано ассоциации HIP. Уведомление REG_REQUIRED имеет тип ошибки 51.

3.3. Обработка запроса регистрации

После запроса регистрации регистратор способен проверить подлинность партнёра на основе отождествления хоста, включённого в пакет I2.

Если регистратору известны отождествления HI всех хостов, которые разрешено регистрировать в службе, ему **следует** отклонять регистрацию неизвестных хостов. Однако предварительное указание на регистраторе всех HI может оказаться невозможным, поэтому регистраторам **следует** поддерживать сертификаты HIP [RFC8002] для регистрации на их основе.

Желающему зарегистрироваться заявителю **следует** проверить наличие у себя сертификата для аутентификации у регистратора. Способы получения и определения приемлемости сертификата выходят за рамки этого документа. Если у заявителя имеется подходящие сертификаты, хосту **следует** включить их (или наиболее подходящий) в параметр CERT пакета HIP вместе с параметром REG_REQUEST. Если сертификата у заявителя нет, ему **следует** отправить запрос без параметра CERT для проверки возможности регистрации на основе отождествления HI.

Когда регистратор получает пакет HIP с параметром REG_REQUEST и хотя бы для одного из указанных в параметре типов регистрации требуется проверка подлинности, регистратор **должен** сначала проверить наличие HI заявителя в списке разрешённых для всех типов регистрации из параметра REG_REQUEST. Если заявитель включён в список разрешённых (или регистратору не нужна аутентификация), регистратор **должен** выполнить регистрацию.

Если заявителя нет в списке разрешённых и регистратор требует аутентификации, он **должен** проверить наличие в пакете параметра CERT. При отсутствии параметра регистратор **должен** отклонить регистрацию, требующую проверки подлинности с Failure Type 0 (нуль) - для регистрации нужны свидетельства. Если сертификат имеется и воспринят

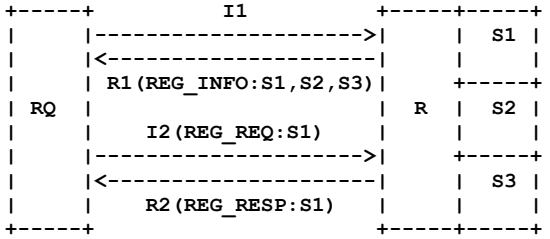
(выпущен для заявителя и подписан доверенным эмитентом), регистратор **должен** выполнить регистрацию. Если сертификат из параметра не подходит, регистратор **должен** отклонить регистрацию и возвратить одну из ошибок:

4 (Bad certificate)
Сертификат повреждён, содержит недействительные подписи и т. п.
5 (Unsupported certificate)
Сертификат неподдерживаемого типа.
6 (Certificate expired)
Срок действия сертификата истёк.
7 (Certificate other)
Сертификат не удалось проверить по какой-либо не указанной причине.
8 (Unknown CA)
Удостоверяющий центр (CA), выпустивший сертификат, не удалось найти или к нему нет доверия.

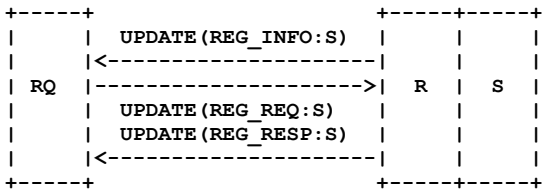
После успешной проверки подлинности регистратор включает в отклик параметр REG_RESPONSE, указывающий тип служб, для которых выполнена регистрация, а также может включать параметры REG_FAILED с указанием служб, для которых регистрация не разрешена или произошёл отказ при попытке регистрации. Отклик может размещаться в пакете R2 или сообщении UPDATE в зависимости от запроса регистрации при базовом согласовании или после создания ассоциации. Параметр REG_FAILED с нулевым значением Failure Type указывает типы служб, регистрация в которых требует дополнительного свидетельства (credential).

Если регистратору нужна дополнительная проверка полномочий и у заявителя имеются нужные свидетельства, ему **следует** попытаться повторить регистрацию в службе после создания ассоциации HIP.

Успешная обработка параметра REG_RESPONSE создаёт состояние регистрации у заявителя. Успешная обработка параметра REG_REQUEST создаёт состояние регистрации у регистратора и, возможно, в службе. Заявитель и регистратор могут отменить регистрацию до завершения срока её действия, если предоставляемые регистрацией услуги больше не нужны заявителю или не могут обеспечиваться регистратором (например, при смене конфигурации).



На рисунке показано, как заявитель (RQ) регистрируется для служба (S1) на регистраторе (R) служб (S1), (S2), (S3) с которым у него нет ассоциации HIP.



На рисунке показано, как заявитель (RQ) регистрируется для службы (S) на регистраторе (R) служб (S), с которым у него имеется ассоциация HIP.

4. Формат и обработка параметров

В этом разделе описан формат и обработка новых параметров, добавляемых расширением HIP Registration. Представление параметров соответствует формату HIPv2 TLV, описанному в параграфе 5.2.1 RFC7401 [RFC7401].

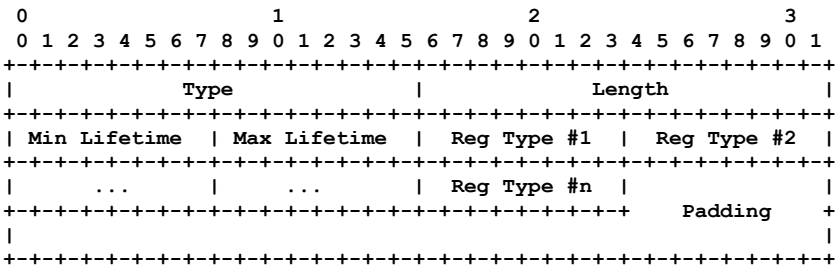
4.1. Представление срока регистрации

При регистрации HIP применяется экспоненциальное представление срока действия регистрации.

Специальное значение 0 (нуль) в поле срока действия **должно** считаться сроком продолжительностью 0 секунд и служит для запроса и подтверждения отмены регистрации.

Ненулевые значения в поле lifetime, используемые в этом документе **должны** интерпретироваться как показатель степени для вычисления срока действия по формуле $2^{((\text{lifetime} - 64)/8)}$ (в секундах). Это позволяет компактно задавать срок действия 255 различными значениями (в дополнение к специальному значению 0) от $2^{(63/8)}$ (~4 мсек) до $2^{(191/8)}$ (~178 дней) 8-битового целого числа без знака.

4.2. REG_INFO



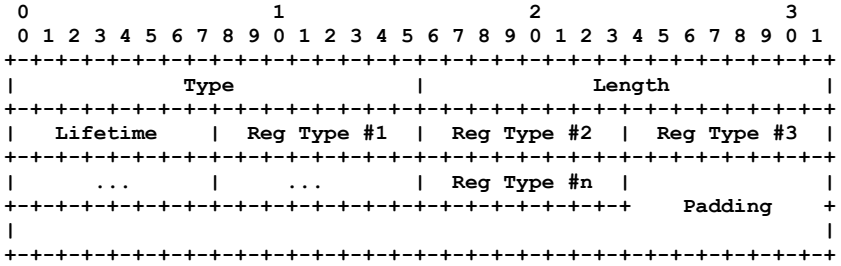
Type
930

Length
Размер в октетах с учётом полей Type, Length, Padding.
Min Lifetime
Минимальный срок регистрации.
Max Lifetime
Максимальный срок регистрации.
Reg Type
Типы регистрации, предлагаемые регистратором.
Конкретные значения типов регистрации будут заданы в других документах (см. раздел 7).

Регистратор включает параметр в пакеты R1 для анонсирования своих возможностей регистрации. Регистратору **следует** включать параметр в пакеты UPDATE при изменении предлагаемых услуг. Поле HIP_SIGNATURE_2 защищает параметры в пакетах R1.

Регистратор указывает минимальный и максимальный срок регистрации, которые он готов предложить заявителю. Заявителю **не следует** запрашивать регистрацию со сроком действия, выходящим за указанные пределы.

4.3. REG_REQUEST



Type
932
Length
Размер в октетах с учётом полей Type, Length, Padding.
Lifetime
Запрашиваемый срок регистрации.
Reg Type
Типы регистрации в порядке предпочтений.
Конкретные значения типов регистрации будут заданы в других документах (см. раздел 7).

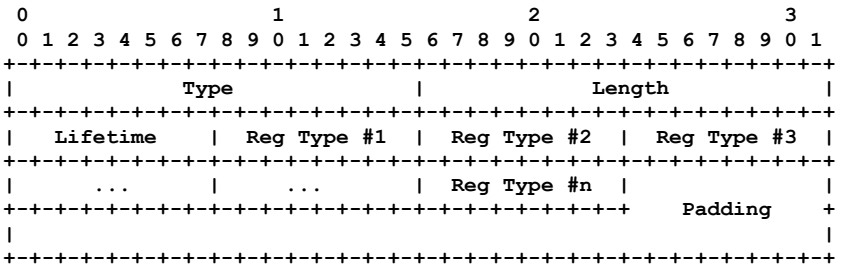
Заявитель включает параметр REG_REQUEST в пакет I2 или UPDATE для регистрации себя. Если параметр REG_REQUEST передан в пакете UPDATE, регистратору **недопустимо** менять регистрации типов, не указанных заявителем. Кроме того, заявителю **недопустимо** включать параметр в пакет, если пакет R1 или последний пакет UPDATE от регистратора не включал параметра REG_INFO с запрашиваемыми типами регистрации.

Заявителю **недопустимо** включать более 1 параметра REG_REQUEST в пакет I2 или UPDATE, а регистратор **должен** быть способен обработать 1 или несколько параметров REG_REQUEST в принимаемых пакетах I2 и UPDATE.

При получении регистратором запроса со сроком меньше или больше указанного им в REG_INFO, ему **следует** установить минимальный или максимальный срок, соответственно.

Поле HIP_SIGNATURE_2 защищает параметры в пакетах I2 и UPDATE.

4.4. REG_RESPONSE



Type
934
Length
Размер в октетах с учётом полей Type, Length, Padding.
Lifetime
Предоставленный срок регистрации.
Reg Type
Предоставленные типы регистрации в порядке предпочтений.
Конкретные значения типов регистрации будут заданы в других документах (см. раздел 7).

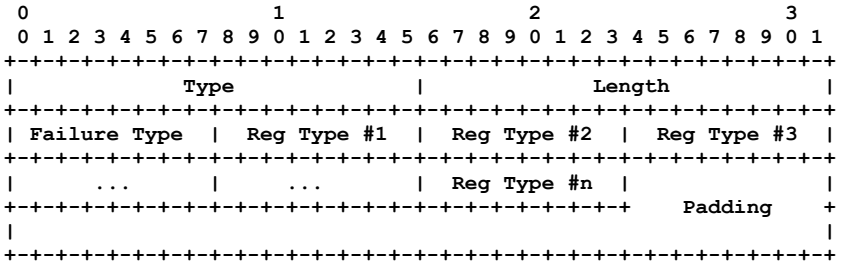
Регистратору **следует** включать параметр REG_RESPONSE в пакет R2 или UPDATE лишь при успешной регистрации.

Регистратору **недопустимо** включать долее 1 параметра REG_RESPONSE в сообщение R2 или UPDATE, а заявитель **должен** быть способен обработать 1 или несколько параметров REG_RESPONSE в принятом пакете R2 или UPDATE.

Заявитель **должен** быть готов получить любой срок регистрации, включая минимум и максимум, указанные в параметре REG_INFO. **Недопустимо** считать, что назначенный срок совпадёт с запрошенным, даже если запрошено время из указанного регистратором интервала.

Поле HIP_SIGNATURE_2 защищает параметры в пакетах R2 и UPDATE.

4.5. REG_FAILED



Type

936

Length

Размер в октетах с учётом полей Type, Length, Padding.

Failure Type

Причина отказа.

Reg Type

Типы регистрации, в которых было отказано по указанной причине.

Значение	***Тип отказа при регистрации***
0	Для регистрации нужны дополнительные свидетельства (credential)
1	Тип регистрации недоступен
2	Недостаточно ресурсов
3	Недействительный сертификат
9-200	Не выделены
201-255	Зарезервированы для приватного использования

Конкретные значения типов регистрации будут заданы в других документах (см. раздел 7).

Failure Type 0 (нуль) указывает, что требуются дополнительные свидетельства (credential) для предоставления заявителю запрошенных параметром типов регистрации. Failure Type 1 (один) указывает, что регистратор не поддерживает запрошенный тип. Failure Type 2 указывает, что у регистратора в данный момент недостаточно ресурсов для запрошенной заявителем регистрации. В таких случаях заявителю **недопустимо** сразу же повторять попытку, но он **может** воспользоваться другим регистратором. Failure Type 3 говорит, что регистратор не может подтвердить действительность представленного заявителем сертификата и в этом случае заявителю **недопустимо** повторять попытку с тем же сертификатов, но он **может** предпринять попытку регистрации для того же набора услуг с другим сертификатом или иного набора услуг с тем же сертификатом.

Регистратору **следует** включать параметр REG_FAILED в пакет R2 или UPDATE, если регистрация с указанными заявителем типами завершилась отказом и заявителю предлагается повторить попытку с предоставлением дополнительных свидетельств.

Поле HIP_SIGNATURE_2 защищает параметры в пакетах R2 и UPDATE.

5. Организация и поддержка регистрации

Организация и/или поддержка регистрации может потребовать дополнительных сведений, не представленных в параметре REG_REQUEST или REG_RESPONSE. Поэтому тип регистрации **может** задавать зависимости для параметров HIP, не указанные в этом документе. Их семантика определяется соответствующей спецификацией типа регистрации.

Заявитель и регистратор **должны** поддерживать минимальный срок регистрации 10 секунд и им **следует** поддерживать максимальный срок не менее 120 секунд. Эти значения задают базовый уровень для спецификации услуг на основе системы регистрации. Значения были выбраны не слишком короткими и не слишком длинными, чтобы учитывать существующие тайм-ауты состояний в промежуточных устройствах (например, NAT и межсетевых экранах).

Нулевой срок регистрации зарезервирован для отмены. Запрос нулевого срока для типа регистрации эквивалентен отмене регистрации для этого типа. Заявитель **может** отменить регистрации до завершения её срока, передав регистратору REG_REQ с нулевым сроком действия. Регистратору **следует** отвечать на запрос, предоставляя регистрацию со сроком действия 0. Регистратор (и подключённое устройство) **может** по своему усмотрению отменить регистрацию до завершения её срока. Однако в таком случае ему **следует** передать REG_RESPONSE с нулевым сроком действия всем зарегистрированным заявителям.

6. Вопросы безопасности

В этом разделе рассматриваются угрозы для протокола регистрации HIP и их влияние на безопасность HIP в целом. Показано, что описанные в этом документе расширения не создают дополнительных угроз для протокола HIP.

Описанные в документе расширения основаны на базовом обмене HIP и не меняет его защитных свойств, например, цифровых подписей или хэшированных кодов аутентификации сообщений (Hashed Message Authentication Code или HMAC). Поэтому единственной угрозой, связанной с этими расширениями является создание программного состояния регистрации на стороне регистратора.

Регистраторы действуют на добровольной основе и вольны выбрать роль ответчика, а затем создавать ассоциации HIP со множеством возможно неизвестных хостов. Поскольку они в любом случае хранят состояние ассоциации, добавление некоторого числа ограниченных по сроку действия состояний регистрации HIP не должно вносить серьёзных дополнительных угроз, особенно благодаря тому, что регистратор HIP может в любой момент по своему усмотрению отменить регистрацию, например, в случае нехватки ресурсов, возникшей в результате атаки.

7. Взаимодействие с IANA

Этот раздел следует трактовать в соответствии с «Guidelines for Writing an IANA Considerations Section in RFCs» [RFC5226].

В [RFC5203], отменённом этим документом, заданы определения и резервирование указанных в таблице типов в субреестре Parameter Types реестра Host Identity Protocol (HIP) Parameters.

Значение	*Тип параметра*	*Размер*
930	REG_INFO	Переменный
932	REG_REQUEST	Переменный
934	REG_RESPONSE	Переменный
936	REG_FAILED	Переменный

В субреестре Parameter Types реестра Host Identity Protocol (HIP) Parameters ссылки на отменённый документ [RFC5203] заменены ссылками на данный документ.

В [RFC5203], отменённом данным документом, запрошено создание субреестра Registration Types в реестре Host Identity Protocol (HIP) Parameters, но не задано типов регистрации. Данный документ резервирует указанные в таблице типы.

Reg Type (тип регистрации)	*Служба*
201-255	Зарезервированы IANA для приватного использования

Для добавления нового типа требуется спецификация IETF.

В субреестре Registration Types реестра Host Identity Protocol (HIP) Parameters ссылки на отменённый документ [RFC5203] заменены ссылками на данный документ.

В [RFC5203], отменённом данным документом, запрошено создание субреестра Registration Failure Types в реестре Host Identity Protocol (HIP) Parameters с включением указанных в таблице определений и резервирования.

Тип отказа	*Причина*
0	Для регистрации требуются дополнительные свидетельства
1	Тип регистрации недоступен
201-255	Зарезервированы IANA для приватного использования

Для добавления нового типа требуется спецификация IETF.

В субреестре Registration Failure Types реестра Host Identity Protocol (HIP) Parameters ссылки на отменённый документ [RFC5203] заменены ссылками на данный документ и добавлены указанные в таблице коды отказов.

Значение	*Тип отказа при регистрации*	
2	Insufficient resources	Недостаточно ресурсов
3	Invalid certificate	Недействительный сертификат
4	Bad certificate	Неприемлемый (плохой) сертификат
5	Unsupported certificate	Неподдерживаемый сертификат
6	Certificate expired	Просроченный сертификат
7	Certificate other	Другая проблема с сертификатом
8	Unknown CA	Неизвестный УЦ
201-255	Reserved for Private Use	Резерв для приватного использования

8. Литература

8.1. Нормативные документы

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

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <http://www.rfc-editor.org/info/rfc7401>.

[RFC8002] Heer, T. and S. Varjonen, "Host Identity Protocol Certificates", RFC 8002, DOI 10.17487/RFC8002, October 2016, <http://www.rfc-editor.org/info/rfc8002>.

[RFC8004] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", RFC 8004, DOI 10.17487/RFC8004, October 2016, <http://www.rfc-editor.org/info/rfc8004>.

8.2. Дополнительная литература

[HIP-ARCH] Moskowitz, R. and M. Komu, "Host Identity Protocol Architecture", Work in Progress[1], draft-ietf-hip-rfc4423-bis-14, June 2016.

[HIP-NAT] Keranen, A., Melen, J., and M. Komu, "Native NAT Traversal Mode for the Host Identity Protocol", Work in Progress, draft-ietf-hip-native-nat-traversal-13[2], July 2016.

[RFC3234] Carpenter, B. and S. Brim, "Middleboxes: Taxonomy and Issues", RFC 3234, DOI 10.17487/RFC3234, February 2002, <http://www.rfc-editor.org/info/rfc3234>.

[RFC5203] Laganier, J., Koponen, T., and L. Eggert, "Host Identity Protocol (HIP) Registration Extension", RFC 5203, DOI 10.17487/RFC5203, April 2008, <http://www.rfc-editor.org/info/rfc5203>.

[1]Опубликовано в RFC 9063. *Прим. перев.*
[2]Опубликовано в RFC 9028. *Прим. перев.*

Приложение A. Отличия от RFC 5203

- Обновлены ссылки с указанием пересмотренных спецификаций HIP.
- Добавлено значение Failure Type для случая нехватки ресурсов, доступных регистратору HIP.
- Добавлена аутентификация заявителя на основе сертификатов и новые значения Failure Type для недействительных сертификатов.

Благодарности

Указанные в алфавитном порядке люди представили содержательные и полезные замечания и/или предложения для улучшения этого документа: Jeffrey Ahrenholz, Miriam Esteban, Ari Keranen, Mika Kousa, Pekka Nikander, Hannes Tschofenig.

Lars Eggert получил финансирование в рамках исследовательской и инновационной программы Европейского союза Horizon 2020 на 2014-2018 годы по гранту № 644866. Этот документ отражает лишь точку зрения авторов и Европейская комиссия не несёт ответственности за какое-либо использование содержащихся в документе сведений.

Ari Keranen предложил включить текст, определяющий предоставление полномочий заявителю на основе сертификатов, как прямую адаптацию текста из спецификации работы HIP через трансляторы NAT [HIP-NAT].

Спасибо Joel M. Halpern за рецензирование Gen-ART для этого документа в процессе его публикации.

Участники работы

Teemu Koponen был соавтором ранней экспериментальной версии этой спецификации [RFC5203].

Адреса авторов

Julien Laganier
Luminate Wireless, Inc.
Cupertino, CA
United States of America
Email: julien.ietf@gmail.com

Lars Eggert
NetApp
Sonnenallee 1
Kirchheim 85551
Germany
Phone: +49 151 12055791
Email: lars@netapp.com
URI: http://eggert.org

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru