Internet Engineering Task Force (IETF)
Request for Comments: 9257
Category: Informational
ISSN: 2070-1721

R. Housley
Vigil Security
J. Hoyland
Cloudflare Ltd.
M. Sethi
Aalto University
C. A. Wood
Cloudflare

July 2022

Guidance for External Pre-Shared Key (PSK) Usage in TLS

Рекомендации по применению внешних PSK в TLS

Аннотация

В этом документе приведены рекомендации по использованию внешних, заранее распределенных ключей (Pre-Shared Key или PSK) в защите транспортного уровня (Transport Layer Security или TLS) версии 1.3, определённой в RFC 8446. Указаны свойства защиты TLS, обеспечиваемые PSK с некоторыми допущениями, и показано, как нарушение этих предположений ведёт к атакам. Даны рекомендации для приложений, помогающие соблюсти эти допущенияю В документе также обсуждаются примеры использования PSK и процессы предоставления, а также указаны свойства защиты и приватности, которые не обеспечиваются TLS 1.3 при использовании внешних PSK.

Статус документа

Документ не относится к категории Internet Standards Track и публикуется лишь для информации.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Не все одобренные IESG документы являются кандидатами в Internet Standard, см раздел 2 RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc9257.

Оглавление

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

1. Введение

В этом документе представлены рекомендации по использованию внешних ключей PSK в TLS 1.3 [RFC8446], применимые также к протоколам Datagram TLS (DTLS) 1.3 [RFC9147] и Compact TLS 1.3 [CTLS]. Для удобочитаемости все они обозначаются в документе как TLS.

Внешние PSK являются симметричными секретными ключами, предоставляемыми реализации протокола TLS извне. Внешние PSK обеспечиваются не через сеть (по внешнему каналу - out of band).

Документ перечисляет защитные свойства TLS, обеспечиваемые PSK при некоторых допущениях, и показывает, как нарушение этих предположений ведёт к атакам. В документе рассматриваются примеры использования PSK, процессы представления и поддержка реализации стека TLS в контексте этих допущений. Документ также предлагает варианты применения, способствующие соблюдению этих допущений.

Имеется много ресурсов с рекомендациями по созданию и проверке паролей в целях повышения защищенности. Однако эквивалентных документов для внешних PSK в TLS нет и здесь этот пробел заполняется.

2. Уровни требований

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

3. Обозначения

В этом документе логическим узлом (logical node) считается вычислительная сущность (computing presence), с которой другие стороны могут взаимодействовать по протоколу TLS. Логический узел может быть реализован в форме нескольких физических экземпляров (объектов) с единым административным управлением, например, серверной фермы. Конечной точкой (endpoint) называется клиент или сервер, участвующий в соединении.

4. Свойства безопасности PSK

Использование заранее созданных PSK позволяет узлам TLS проверить подлинность отождествлений конечных точек, а также обеспечивает другие преимущества, такие как устойчивость к атакам в присутствии квантовых компьютеров (см. параграф 4.2). Однако эти ключи не обеспечивают защиту приватности (конфиденциальности) отождествлений конечных точек и неотказуемость (одна из точек соединения может отвергнуть диалог), как отмечено в разделе 7.

безопасность аутентификации PSK предполагает одно фундаментальное свойство - каждый ключ PSK известен лишь одному клиенту и одному серверу, которые никогда не меняются ролями. Если это нарушается, защитные свойства TLS существенно ухудшаются, как показано ниже.

4.1. Совместное использование PSK

Как обсуждается в параграфе 5.1 для демонстрации атаки, [AASS19] описывает сценарии, где один ключ PSK используется множеством клиентов и множеством серверов. Если по наивности общий ключ предоставлен всем членам группы, TLS проверяет лишь принадлежность к группе и безопасность системы в целом становится достаточно слабой. Здесь имеется ряд указанных ниже недостатков.

1. Любой член группы может выдать себя за другого члена этой группы.
2. Если PSK комбинируется с результатом обмена свежими эфемерными ключами, компрометация члена группы, знающего общий секрет, приводит к доступности этого секрета злоумышленнику для пассивного чтения трафика (и активного его изменения).
3. Если PSK не комбинируется с результатом обмена свежими эфемерными ключами, компрометация члена группы, знающего общий секрет, приводит к доступности этого секрета злоумышленнику для пассивного чтения всего трафика, включая прошлый (и активного его изменения).

Кроме того, не входящий в группу злоумышленник может перенаправить согласование между действительными членами группы для их соединения непредусмотренным способом, как описано ниже. Отметим, что возможно частичное смягчение этого класса атак - каждый член группы включает расширение для индикации имени сервера (Server Name Indication или SNI) [RFC6066] и прерывает соединение при насовпадении представленного SNI с известным идентификатором принимающей стороны. Подробности этого представлены в [Selfie].

Для иллюстрации атак с перенаправлением рассмотрим трёх парнтеров (A, B, C), знающих общий ключ PSK. Атака модет иметь вид, представленный ниже.

1. A передаёт ClientHello для B.
2. Атакующий перехватывает сообщение и перенаправляет его C.
3. C отвечает (ServerHello, ...) узлу A.
4. A передаёт сообщение для B, завершая согласования якабы с B.
5. Злоумышленник перенаправляет сообщение Finished узлу to C, что завершает его согласование с A.

В этой атаке проверки подлинности партнёра не происходит. Если C поддерживает более слабый набор шифров, чем B, возможны атаки на снижение (ослабление) криптографического алгоритма. Такое перенаправление является атакой с нарушением привязки отождествления [Krawczyk] [Sethi]. Атака Selfie [Selfie] является особым случаем атаки с перенаправлением против члена группы, который может выступать клиентом и сервером TLS. В этой атаке злоумышленник, не входящий в группу, перенаправляет соединение от клиента к серверу на той же конечной точке.

В дополнение к отмеченным недостаткам общий для узлов ключ PSK может негативно влиять на развёртывание. Например, отзыв отдельных элементов группы становится невозможным без создания нового PSK для оставшихся.

4.2. Энтропия PSK

Свойства энтропии внешних PSK также могут влиять на защитные свойства TLS. Например, при использовании PSK с высокой энтропией режимы организации только ключей PSK обеспечивают ожидаемые защитные свойства TLS, включая организацию одного сеансового ключа между партнёрами, секретность сеансовых ключей, проверку подлинности партнёров и защиту от снижения версии. Разъяснение этих свойств дано в приложении E.1 к [RFC8446]. Однако этим режимам не достает полной защиты (forward security), которая может быть достигнута при использовании режима PSK-DH или краткосрочных PSK.

При использовании PSK с малой энтропией режимы организации только ключей PSK подвержены пассивным атакам с исчерпывающим поиском, которые раскрывают ключи трафика. режимы PSK-DH подвержены активным атакам, в которых злоумышленник выдаёт себя за одну сторону. Фаза исчерпывающего поиска в этих атаках может быть организована в автономном режиме (offline) если атакующий перехватывает одно согласование с применением PSK, но такие атаки не ведут к раскрытию ключей трафика для данного соединения, поскольку ключи зависят также от обмена Диффи-Хеллмана (Diffie-Hellman или DH). Ключи с малой энтропией защизены от активных атак, если с TLS применяется обмен ключами с парольной аутентификацией (Password-Authenticated Key Exchange или PAKE). На момент написания этого документа исследовательская группа Crypto Forum (Crypto Forum Research Group илиCFRG) занималась подготовкой спецификации, рекомендуемых PAKE ([CPACE], [OPAQUE]) для симметричных и асимметричных ключей.

5. Внешние PSK на практике

Шифры PSK были впервые заданы для TLS в 2005 г. Сейчас PSK являются частью спецификации TLS 1.3 [RFC8446]. TLS 1.3 также использует PSK для восстановления сессий. Применяемые для восстановления PSK отличаются от внешних PSK, которые представляются по отдельному каналу (out of band0. В этой спецификации описаны известные варианты применения и процессы представляния для внешних PSK в TLS.

5.1. Примеры использования

В этом параграфе даны некоторые варианты применения, где парные внешние ключи PSK (внешние PSK, совместно применяемые одним клиентом и одним сервером) применяются для аутентификации в TLS. Порядок примеров не отражает каких-либо приоритетов.

Взаимодействие между устройствами с синхронизацией ключей по отдельному каналу
: PSK предоставляются по отдельному каналу (out of band) для взаимодействия с известными отождествлениями, при этом отождествление раскрывается через другой online-протокол.

Коммуникации внутри ЦОД
: Межмашинное взаимодействие в одном центре обработки данных (ЦОД) или точке присутствия (Point of Presence или PoP) может использовать представленные извне PSK. Это применяется в основном для поддержки соединений TLS с упреждающими данными (early data). Соображения об использовании упреждающих данных с внешними PSK представлены в разделе 8.

Межсерверное взаимодействие без сертификатов
: При межмашинном взаимодействии могут применяться предоставленные извне PSK. Это служит в основном для организации соединений TLS без издержек на предоставление и поддержку сертификатов PKI.

Интернет вещей (IoT) и устройства с ограниченными вычислительными возможностями
: [RFC7925] задаёт профили TLS и DTLS для устройств с ограниченными ресурсами и предлагает применять шифры PSK для совместимых устройств. Спецификация LwM2M (Open Mobile Alliance Lightweight Machine-to-Machine) [LwM2M] указывает, что серверы LwM2M **должны** поддерживать режим PSK для DTLS.

Защита RADIUS [RFC2865] с помощью TLS
: Шифры PSK не обязательны для этого случая, как указано в [RFC6614].

Аутентификация между пользователем и сервером 3GPP
: Базовая архитектура аутентификации (Generic Authentication Architecture или GAA), заданная в 3GPP, указывает, что шифры TLS PSK можно применять между сервером и оборудованием пользователя для аутентификации [GAA].

Смарт-карты
: Немецкие карты электронной идентификации (German electronic Identity или eID) поддерживают аутентификацию держателя карты в online-службах на основе TLS PSK [SmartCard].

Квантовая устойчивость
: В некоторых развёртывания могут применяться PSK (или их комбинация с аутентификацией на основе сертификатов, как описано в [RFC8773]), благодаря предоставляемой защите от квантовых компьютеров.

Имеются также случаи применения PSK, известных более чем двум объектам. Некоторые примеры приведены ниже (отмечены Ахметзяновой и др. В [AASS19]):

Групповые чаты
: В этом случае участникам группы могут быть предоставлены внешние PSK по отдельному каналу (out of band) для организации аутентифицированных соединений с другими членами группы.

IoT и устройства с ограниченными вычислительными возможностями
: В этом случае возможно много вариантов представления PSK. Например, а данной системе все устройства IoT могут иметь общий ключ PSK и применять его для взаимодействия с центральным сервером (один ключ на n устройств), иметь свои ключи для взаимодействия с центральным сервером (n ключей на n устройств) или иметь парные ключи для вазаимодействия каждого с каждым (n^2 ключей на n устройств).

5.2. Примеры представления

Процесс представления зависит от системных требований и модели угроз. По возможности не следует совместно использовать PSK на узлах, однако иногда этого не избежать. В таких случаях следует использовать рекомендации, приведённые в разделе 6. Ниже приведены примеры процессов представления PSK.

- Многие промышленные протоколы предполагают, что PSK распределяются и назначаются вручную путём (1) прямого ввода PSK в устройство или (2) использования доверенного при первом применении (trust-on-first-use или TOFU) подхода, когда устройство совсем не защищено до первого входа в систему (login). Многие устройства имеют очень ограниченный пользовательский интерфейс (UI). Например, у них может быть лишь цифровая клавиатура или просто несколько кнопок. Когда подход TOFU не подходит, ключ придётся вводить через ограниченный интерфейс UI.

- Некоторые устройства представляют PSK по особому (out-of-band) протоколу синхронизации на базе облака.

- Некоторые секреты могут быть встроены в аппаратные или программные компоненты устройства. Если это делается во время производства, секреты могут указываться на этикетке или включаться в спецификацию (Bill of Materials) для упрощения сканирования или импорта.

5.3. Ограничения при представлении

Системы представления PSK часто ограничены в зависимости от применения. Например, хотя одной из целей представления является обеспечение уникальности каждой пары ключей, некоторые системы не хотят распространять парные общие ключи для достижения этого. Другим примером служит требование некоторых систем встраивать в процессе представления зависимую от приложения информацию в PSK или иные отождествления. Для отождествлений иногда может требоваться маршрутизация, что в настоящее время обсуждается [EAP-TLS-PSK].

6. Рекомендации по использованию внешних PSK

1. При выводе каждого PSK **следует** обеспечивать хотя бы 128 битов энтропии, ключ **должен** быть не короче 128 битов и его **следует** комбинировать с обменом эфемерными ключами, например, с использованием psk_dhe_ke (Pre-Shared Key Exchange Mode) в TLS 1.3 для полной защиты. Как обсуждалось в разделе 4, PSK с низкой энтропией (т. е. выведенные с использованием менее 128 битов энтропии) подвержены атакам и их **следует** избегать. Если доступны лишь ключи с малой энтропией, **следует** применять механизмы организации ключей вроде PAKE, которые могут снизить риск offline-атак по словарю. Отметим, что такие механизмы ещё не стандартизованы и не обязательно будут следовать той же архитектуре, что и процесс встраивания внешних ключей PSK, описанный в [RFC9258].

2. Если не принято иных мер по снижению риска для PSK, известных группе, использование каждого PSK **должно** ограничиваться не более чем двумя логическими узлами, один из которых играет роль сервера, другой - роль клиента TLS (логические узлы **могут** совпадать в разных ролях). В [RFC9258] описаны две меры снижения риска: (1) обмен идентификаторами клиента и сервера через соединение TLS после согласования и (2) встраивание идентификаторов клиента и сервера в строку контекста для импортёра внешнего PSK.

3. Узлам **следует** импользовать импортёров внешних PSK [RFC9258] при настройке PSK для пары клиент-сервер, когда это возможно. Импортёры упрощают представление внешних PSK и делают их меньше подверженными ошибкам, выводя уникальный импортируемый PSK из внешнего PSK для каждой поддерживаемом узлом функции вывода ключей (см. раздел «Вопросы безопасности» в [RFC9258]).

4. По возможности основной ключ PSK (передаваемый импортёру) **следует** удалять после генерации импортируемых ключей. Это не позволит злоумышленнику использовать компрометацию одного узла для атак на соединения между любыми узлами. Иначе атакующий сможет восстановить основной ключ и снова запустить импортёр.

6.1. Интерфейс стека

Большинство основных реализаций TLS поддерживает внешние PSK. Стеки с поддержкой внешних PSK предоставляют интерфейс, который приложения могут использовать при настройке PSK для отдельных соединений. Детали некоторых имеющихся на момент написания документа стеков приведены ниже.

OpenSSL и BoringSSL
: Приложения могут указать поддержку внешних PSK через отдельные шифры в TLS 1.2 и ниже. Они также могут настроить обратные вызовы (callback) для выбора PSK при согласовании. Эти вызовы должны обеспечивать ключ и отождествление PSK. Точный формат обратного вызова зависит от согласованной версии протокола TLS, новые функции обратного вызова специально добавлены в OpenSSL для TLS 1.3 [RFC8446] с поддержкой PSK. Размер PSK проверяется на диапазон 1-256 байтов (включительно), отождествление может иметь размер до 128 байтов.

mbedTLS
: Клиентские приложения настраивают PSK до создания соединения путём предоставления встроенного отождествления и значения PSK. Серверы должны реализовать обратные вызовы как в OpenSSL. Отождествление и ключ PSK могут иметь размер от 1 до 16 байтов (включительно).

gnuTLS
: Приложения настраивают PSK как необработанные (raw) строки байтов или шестнадцатеричные строки. Отождествление и ключ PSK не проверяются.

wolfSSL
: Приложения настраивают PSK с обратными вызовами, подобно OpenSSL.

6.1.1. Кодирование и сравнение отождествлений PSK

Параграф 5.1 в [RFC4279] указывает, чтобы отождествление PSK сначала следует преобразовать в строку символов, а затем кодировать в октеты с применением UTF-8. Это делается для предотвращения проблем совместимости (особено при понятных человеку отождествлениях). С другой стороны, [RFC7925] рекомендует реализациям не применять структурированные форматы для отождествлений PSK и выполнять побайтовое сравнение при любых операциях. При ручной настройке отождествлений PSK важно помнить, что визуально идентичные строки могут отличаться кодировкой.

TLS 1.3 [RFC8446] следует той же практике задания отождествлений PSK последовательностью не обрабатываемых байтов (opaque identity<1..2^{16}-1> в спецификации), которые сравниваются побайтово. [RFC8446] требует отождествлений PSK не короче 1 1 и не длиннее 65535 байтов. Хотя [RFC8446] не задаёт строгих требований к формату отождествлений, этот формат может быть разным в зависимости от развёртывания, как указано ниже.

- Отождествление PSK **может** быть задаваемой пользователем строкой при использовании с такими протоколами как EAP (Extensible Authentication Protocol) [RFC3748]. Например, gnuTLS считает отождествления PSK именами пользователей.
- Отождествления PSK **могут** включать суффикс доменного имени для роуминга и объединения. В приложениях и установках, где суффикс домена считается конфиденциальным, такая практика **не рекомендуется**.
- При развёртывании следует озаботиться, чтобы размер отождествления позволял предотвратить конфликты.

6.1.2. Конфликты отождествлений PSK

Возможны, хоть и маловероятны, конфликты отождествлений внеших PSK с отождествлениями PSK возобновления. Реализация стека TLS и последовательность обратных вызовов влияют на поведение приложений в случае конфликта. При получении сервером отождествления PSK в TLS 1.3 ClientHello, некоторые стеки TLS выполняют зарегистрированный приложением обратный вызов до проверки кэша возобновления сессий в стеке. Это значит, что при конфликте отождествлений использование внешнего PSK обычно становится предпочтительней восстановления. Поскольку отождествления PSK для восстановления задаёт реализация стека TLS, **рекомендуется** выделять эти значения так, чтобы можно было отличить PSK возобновления от внешних PSK во избежание конфликтов.

7. Вопросы приватности

Свойства конфиденциальности PSK ортогональны свойствам безопасности, описанным в разделе 4. TLS мало заботится о приватности отождествлений PSK. Например, получает сведения о внешнем PSK или его отождествлении за счёт того, что отождествление открыто передаётся в ClientHello. В результате пассивный противник может связать несколько соединений, использующих один внешний PSK в линии. В зависимости от отождествления PSK пассивный атакующий может также идентифицировать устройство, персону или предприятие, использующее клиент или сервер TLS. Активный злоумышленник может также применить отождествление PSK для помех согласованию или данным приложения от конкретного устройства путём блокировки, задержки или ограничения скорости трафика. Методы снижения таких рисков требуют дополнительного анализа и выходят за рамки документа. Кроме сопоставления устройств в сети внешние PSK по своей природе связаны получателями PSK. В частности, сервер может связывать друг с другом последовательные соединения с одним внешним PSK. Предотвращение этого выходит за рамки документа.

8. Вопросы безопасности

Этот документ посвящён вопросам безопасности. Следует повторить, что имеются опасения, связанные с применением внешних PSK в части подобающей идентификации конечных точек TLS 1.3 и дополнительных рисков при известности внешних PSK группе узлов.

Не рекомендуется применять один ключ PSK более чем на одном клиенте и одном сервере. Однако, как отмечено в параграфе 5.1, имеются приложения, опирающиеся на использование одного PSK множеством узлов. [RFC9258] помогает смягчить перенаправление и отражение в стиле Selfie при использовании одного PSK на множестве узлов. Это достигается корректным применением идентификаторов узлов в конструкции ImportedIdentity.context [RFC9258]. Одним из решений служит выбор каждой конечной точкой одного глобально уникального идентификатора для всех согласования PSK. Таким идентификатором может служить, например, один из MAC-адресов (Media Access Control) точки, 32-битовое случайное значение или UUID (Universally Unique IDentifier) [RFC4122]. Отметим, что такие почтоянные идентификаторы влияют на приватность (см. раздел 7). Каждой конечной точке **следует** знать идентификатор точки, с которой нужно соединиться и **следует** сравнивать его с идентификатором из ImportedIdentity.context. Важно помнить, что конечные точки с одним групповым PSK могут представляться друг другом.

Соображения по использованию внешних PSK не ограничиваются верной идентификацией. При использовании упреждающих данных с внешним PSK случайное значение в ClientHello является единственным источником энтропии, способствующим смене ключей между сессиями. В результате при неоднократном применении внешнего PSK источник случайных значений у клиента играет важную роль в защите упреждающих данных.

9. Взаимодействие с IANA

Этот документ не требует действий IANA.

10. Литература

10.1. 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, <https://www.rfc-editor.org/info/rfc2119>.

[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>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC9258] Benjamin, D. and C. A. Wood, "Importing External Pre-Shared Keys (PSKs) for TLS 1.3", RFC 9258, DOI 10.17487/RFC9258, July 2022, <https://www.rfc-editor.org/info/rfc9258>.

10.2. Дополнительная литература

[AASS19] Akhmetzyanova, L., Alekseev, E., Smyshlyaeva, E., and A. Sokolov, "Continuing to reflect on TLS 1.3 with external PSK", April 2019, <https://eprint.iacr.org/2019/421.pdf>.

[CPACE] Abdalla, M., Haase, B., and J. Hesse, "CPace, a balanced composable PAKE", Work in Progress, Internet-Draft, draft-irtf-cfrg-cpace-06, 24 July 2022, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-cpace-06>.

[CTLS] Rescorla, E., Barnes, R., Tschofenig, H., and B. M. Schwartz, "Compact TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-ctls-06, 9 July 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-ctls-06>.

[EAP-TLS-PSK] Mattsson, J. P., Sethi, M., Aura, T., and O. Friel, "EAP-TLS with PSK Authentication (EAP-TLS-PSK)", Work in Progress, Internet-Draft, draft-mattsson-emu-eap-tls-psk-00, 9 March 2020, <https://datatracker.ietf.org/doc/html/draft-mattsson-emu-eap-tls-psk-00>.

[GAA] ETSI, "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Generic Authentication Architecture (GAA); System description", version 12.0.0, ETSI TR 133 919, October 2014, <https://www.etsi.org/deliver/etsi_tr/133900_133999/133919/12.00.00_60/tr_133919v120000p.pdf>.

[Krawczyk] Krawczyk, H., "SIGMA: The 'SIGn-and-MAc' Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols", DOI 10.1007/978-3-540-45146-4_24, 2003, <https://link.springer.com/content/pdf/10.1007/978-3-540-45146-4_24.pdf>.

[LwM2M] Open Mobile Alliance, "Lightweight Machine to Machine Technical Specification", version 1.0, February 2017, <http://www.openmobilealliance.org/release/LightweightM2M/V1_0-20170208-A/OMA-TS-LightweightM2M-V1_0-20170208-A.pdf>.

[OPAQUE] Bourdrez, D., Krawczyk, H., Lewi, K., and C. A. Wood, "The OPAQUE Asymmetric PAKE Protocol", Work in Progress, Internet-Draft, draft-irtf-cfrg-opaque-09, 6 July 2022, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-opaque-09>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/info/rfc2865>.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, DOI 10.17487/RFC3748, June 2004, <https://www.rfc-editor.org/info/rfc3748>.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/info/rfc4122>.

[RFC4279] Eronen, P., Ed. and H. Tschofenig, Ed., "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, DOI 10.17487/RFC4279, December 2005, <https://www.rfc-editor.org/info/rfc4279>.

[RFC6066] Eastlake 3rd, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, DOI 10.17487/RFC6066, January 2011, <https://www.rfc-editor.org/info/rfc6066>.

[RFC6614] Winter, S., McCauley, M., Venaas, S., and K. Wierenga, "Transport Layer Security (TLS) Encryption for RADIUS", RFC 6614, DOI 10.17487/RFC6614, May 2012, <https://www.rfc-editor.org/info/rfc6614>.

[RFC7925] Tschofenig, H., Ed. and T. Fossati, "Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things", RFC 7925, DOI 10.17487/RFC7925, July 2016, <https://www.rfc-editor.org/info/rfc7925>.

[RFC8773] Housley, R., "TLS 1.3 Extension for Certificate-Based Authentication with an External Pre-Shared Key", RFC 8773, DOI 10.17487/RFC8773, March 2020, <https://www.rfc-editor.org/info/rfc8773>.

[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>.

[Selfie] Drucker, N. and S. Gueron, "Selfie: reflections on TLS 1.3 with PSK", DOI 10.1007/s00145-021-09387-y, May 2021, <https://eprint.iacr.org/2019/347.pdf>.

[Sethi] Sethi, M., Peltonen, A., and T. Aura, "Misbinding Attacks on Secure Device Pairing and Bootstrapping", DOI 10.1145/3321705.3329813, May 2019, <https://arxiv.org/pdf/1902.07550>.

[SmartCard] Bundesamt für Sicherheit in der Informationstechnik, "Technical Guideline TR-03112-7 eCard-API-Framework - Protocols", version 1.1.5, April 2015, <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03112/TR-03112-api_teil7.pdf?__blob=publicationFile&v=1>.

Благодарности

Этот документ является результатом работы TLS External PSK Design Team, включающей Benjamin Beurdouche, Björn Haase, Christopher Wood, Colm MacCarthaigh, Eric Rescorla, Jonathan Hoyland, Martin Thomson, Mohamad Badra, Mohit Sethi, Oleg Pekar, Owen Friel, Russ Housley.

Документ был улучшен, благодаря высококачественным рецензиям Ben Kaduk и John Preuß Mattsson.

Адреса авторов

Russ Housley
Vigil Security, LLC
Email: housley@vigilsec.com

Mohit Sethi
Aalto University
Email: mohit@iki.fi

Jonathan Hoyland
Cloudflare Ltd.
Email: jonathan.hoyland@gmail.com

Christopher A. Wood
Cloudflare
Email: caw@heapingbits.net

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru