Internet Engineering Task Force (IETF) N. Mavrogiannopoulos
Request for Comments: 6091 KUL
Obsoletes: 5081 D. Gillmor
Category: Informational Independent
ISSN: 2070-1721 February 2011

Использование ключей OpenPGP для аутентификации TLS

Using OpenPGP Keys for Transport Layer Security (TLS) Authentication

Тезисы

Этот документ определяет расширение TLS[1] и связанную с ним семантику, позволяющие клиентам и серверам согласовывать использование сертификатов OpenPGP для сессий TLS, а также задает способ доставки сертификатов OpenPGP через TLS. Документ также определяет реестр для сертификатов, отличных от X.509 типов.

Статус документа

Этот документ не является проектом стандарта Internet и публикуется с информационной целью.

Документ является результатом работы IETF и выражает согласованное мнение сообщества IETF. Документ был представлен на публичное рассмотрение и одобрен для публикации IESG. Не все одобренные IESG документы являются проектами стандартов Internet (см. раздел 2 RFC 5741).

Информацию о текущем статусе документа, обнаруженных ошибках и способах обратной связи можно получить, воспользовавшись ссылкой http://www.rfc-editor.org/info/rfc6091.

Оглавление

1. Введение....1
2. Терминология....1
3. Изменение содержимого сообщений Handshake....2
  3.1. Клиентское сообщение Hello....2
  3.2. Серверное сообщение Hello....2
  3.3. Сертификат сервера....2
  3.4. Запрос сертификата....3
  3.5. Сертификат клиента....3
  3.6. Другие сообщения Handshake....3
4. Вопросы безопасности....3
5. Согласование с IANA....3
6. Благодарности....4
7. Литература....4
  7.1. Нормативные документы....4
  7.2. Дополнительная литература....4
Приложение A. Отличия от RFC 5081....4

1. Введение

IETF имеет два набора стандартов для сертификатов открытых ключей - один использует сертификаты X.509 [RFC5280], а другой — OpenPGP [RFC4880]. Ко времени подготовки этого документа были определены стандарты TLS [RFC5246] для использования сертификатов X.509. Данный документ задает способ согласования использования сертификатов OpenPGP для сессий TLS, а также способ доставки сертификатов OpenPGP с использованием TLS. Предложенные расширения обеспечивают совместимость с существующей спецификацией TLS, поэтому имеющиеся реализации клиентов и серверов, применяющие сертификаты X.509, не затрагиваются этим документом.

Предлагаемые расширения не обеспечивают совместимости с [RFC5081]; основные различия рассмотрены в Приложении A. Хотя значение CertificateType в OpenPGP, используемое в этом документе, совпадает с заданным в [RFC5081], семантика использования отличается. Авторы предполагают, что это различие не вызовет проблем интероперабельности, поскольку реализации [RFC5081] не получили широкого распространения.

2. Терминология

Термин «ключ OpenPGP» используется в этом документе в соответствии со спецификацией OpenPGP [RFC4880]. Для ключей OpenPGP, которые допускается использовать для аутентификации, служит термин «сертификат OpenPGP».

В этом документе используется такая же нотация и терминология, как в спецификации протокола TLS [RFC5246].

[1] Transport Layer Security - защита на транспортном уровне.

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с документом [RFC2119].

3. Изменение содержимого сообщений Handshake

В этом разделе описаны изменения содержимого согласующих сообщений TLS для случая использования сертификатов OpenPGP в целях засвидетельствования.

3.1. Клиентское сообщение Hello

Для индикации поддержки множества типов сертификатов клиенты **должны** включать расширение типа cert_type в расширенное приветственное сообщение (Hello). Расширению TLS cert_type присвоено значение 9 в реестре TLS ExtensionType. Это значение используется в качестве номера расширения для расширений в приветственных сообщениях клиента и сервера. Механизм расширения hello описан в [RFC5246].

Это расширение передает список поддерживаемых типов сертификатов, которые клиент может использовать, отсортированных по уровню предпочтения. Это расширение **должно** опускаться, если клиент поддерживает только сертификаты X.509. Поле extension_data в этом расширении содержит структуру CertificateTypeExtension. Отметим, что структура CertificateTypeExtension используется как клиентом, так и сервером, хотя она описана в документе только один раз. Повторное использование однократно заданной спецификации на клиентской и серверной стороне является общепринятой практикой для спецификаций (в частности, для протокола TLS [RFC5246]).

```
enum { client, server } ClientOrServerExtension;

enum { X.509(0), OpenPGP(1), (255) } CertificateType;

struct {
   select(ClientOrServerExtension) {
      case client:
         CertificateType certificate_types<1..2^8-1>;
      case server:
         CertificateType certificate_type;
   }
} CertificateTypeExtension;
```

Для использования сертификатов OpenPGP не требуется новых шифров. Все существующие шифры, поддерживающие методы обмена ключами, которые совместимы с ключом в сертификате, могут применяться с сертификатами OpenPGP.

3.2. Серверное сообщение Hello

Если сервер получает клиентское сообщение hello, которое содержит расширение cert_type и выбирает шифр, который требует сертификат, возможны два варианта. Сервер **должен** выбрать тип сертификата из поля certificate_types в расширенном приветствии клиента или разорвать сеанс с критическим сигналом типа unsupported_certificate[1].

Выбранный сервером тип сертификата представляется в структуре CertificateTypeExtension, которая включается в расширенное сообщение hello от сервера с использованием расширения типа cert_type. Серверы, поддерживающие только сертификаты X.509, **могут** не включать расширение cert_type в расширенное сообщение hello.

3.3. Сертификат сервера

Содержимое сообщений с сертификатом, передаваемых от сервера клиенту и наоборот, определяется согласованным типом сертификата и алгоритмом обмена ключами выбранного шифра.

Если согласован тип сертификата OpenPGP, требуется представить сертификат OpenPGP в соответствующем сообщении. Сертификат должен включать открытый ключ, который соответствует выбранному алгоритму обмена ключами, как показано в таблице ниже.

Алгоритм обмена ключами	Тип сертификата OpenPGP
RSA	Открытый ключ RSA, который может использоваться для шифрования.
DHE_DSS	Открытый ключ DSA, который может использоваться для аутентификации.
DHE_ RSA	Открытый ключ RSA, который может использоваться для аутентификации.

Сертификат OpenPGP, появляющийся в сообщении, передается с использованием двоичного формата OpenPGP. Сертификат **должен** содержать все элементы, требуемые параграфом 11.1 [RFC4880].

Сертификаты OpenPGP для передачи в сообщении помещаются в структуру Certificate и помечаются типом OpenPGPCertDescriptorType в subkey_cert. Поскольку такие сертификаты могут содержать несколько субключей, идентификатор субключа для использования в данной сессии явно задается в поле OpenPGPKeyID. Идентификатор ключа **должен** быть задан даже в тех случаях, когда сертификат имеет только первичный ключ. Партнер при получении такого типа использует указанный субключ или прерывает сессию с генерацией критического сигнала unsupported_certificate.

Доступна также опция для передачи оттиска OpenPGP взамен передачи сертификата целиком (с помощью тега subkey_cert_fingerprint). Этот тег использует структуру OpenPGPSubKeyFingerprint и требует задания оттиска первичного ключа, а также идентификатора субключа для использования в данной сессии. Партнер будет отвечать критическим сигналом certificate_unobtainable, если сертификат с данным оттиском не будет найден. Критический сигнал certificate_unobtainable определен в разделе 5 [RFC6066].

Реализации этого протокола **должны** гарантировать, что размеры идентификаторов субключей и оттисков в структурах OpenPGPSubKeyCert и OpenPGPSubKeyFingerprint соответствуют требованиям [RFC4880]. Кроме того, **рекомендуется** для ключей, используемых с этим протоколом, устанавливать флаг аутентификации (0x20).

[1] Неподдерживаемый сертификат.

Процесс генерации оттисков описан в параграфе 12.2 [RFC4880].

Перечисляемые типы cert_fingerprint и cert структуры OpenPGPCertDescriptorType, которые были определены в [RFC5081], больше не используются и отменяются данным документом. Тип empty_cert, введенный взамен cert, обеспечивает совместимый с прежней версией способ задания пустого сертификата; использование cert_fingerprint **недопустимо** в соответствии с обновленной спецификацией и, следовательно, старый вариант был удален из описания структуры Certificate.

```
enum {
     empty_cert(1),
     subkey_cert(2),
     subkey_cert_fingerprint(3),
     (255)
} OpenPGPCertDescriptorType;

uint24 OpenPGPEmptyCert = 0;

struct {
    opaque OpenPGPKeyID<8..255>;
    opaque OpenPGPCert<0..2^24-1>;
} OpenPGPSubKeyCert;

struct {
    opaque OpenPGPKeyID<8..255>;
    opaque OpenPGPCertFingerprint<20..255>;
} OpenPGPSubKeyFingerprint;

struct {
     OpenPGPCertDescriptorType descriptorType;
     select (descriptorType) {
          case empty_cert: OpenPGPEmptyCert;
          case subkey_cert: OpenPGPSubKeyCert;
          case subkey_cert_fingerprint:
              OpenPGPSubKeyCertFingerprint;
     }
} Certificate;
```

3.4. Запрос сертификата

Семантика этого сообщения совпадает с определенной в спецификации TLS. Однако, если это сообщение передано и согласован тип OpenPGP, список certificate_authorities **должен** быть пустым.

3.5. Сертификат клиента

Это сообщение передается только в ответ на сообщение с запросом сертификата. Сообщение с сертификатом клиента передается с использованием такого же форматирования, которое служит для сообщений с сертификатом сервера, и также требуется присутствие сертификата, который соответствует согласованному типу. Если были выбраны сертификаты OpenPGP, а у клиента нет нужного сертификата, **должна** передаваться структура сертификата типа empty_cert, которая содержит значение OpenPGPEmptyCert. Серверу в таком случае **следует** отвечать критическим сигналом handshake_failure, если требуется аутентификация клиента.

3.6. Другие сообщения Handshake

Все остальные согласующие сообщения идентичны заданным в спецификации TLS.

4. Вопросы безопасности

Все вопросы безопасности, рассмотренные в [RFC5246], [RFC6066] и [RFC4880], применимы к настоящему документу. Вопросы использования «сети доверия» (web of trust) или верификации тождественности и сертификатов выходят за пределы данного документа. Здесь рассматриваются задачи, обрабатываемые протоколами прикладного уровня.

Протокол для согласования типа сертификата идентичен по своей работе согласованию шифра, описанному в спецификации TLS [RFC5246], с добавлением принятых по умолчанию значений для случаев, когда расширение опущено. Поскольку расширения не задаются крайне редко и к значениям применяется такая же защита, как к выбираемым шифрам, предполагается что уровень защиты совпадает с уровнем защиты при согласовании шифра.

Для случая использования оттисков OpenPGP взамен полных сертификатов применимо обсуждение раздела 5 [RFC6066] для «URL сертификата клиента», особенно при использовании внешних серверов для нахождения ключей. Однако основное различие заключается в том, что расширение client_certificate_url хотя и позволяет идентифицировать сертификаты без включения их хэш-сумм, это невозможно для предложенного здесь использования протокола. В данном протоколе сертификаты, если они не передаются, всегда идентифицируются по их оттискам, которые служат в качестве криптографических хэш-сумм для сертификатов (см. параграф 12.2 [RFC4880]).

Информация, доступная для участвующих сторон и подслушивающих (если ранее не была согласована защита конфиденциальности), включает число и типы сертификатов, а также их содержимое.

5. Согласование с IANA

Этот документ использует реестр cert_type, определенный в [RFC5081]. Имеющиеся в IANA ссылки были обновлены и указывают на настоящий документ.

В дополнение к этому реестр TLS Certificate Types, организованный [RFC5081] был обновлен, как показано ниже.

1. В данном документе определены значения 0 (X.509) и 1 (OpenPGP).

2. Значения из диапазона 2 - 223, включительно, выделяются в соответствии с процедурой RFC Required [RFC5226].
3. Значения из диапазона 224 - 255, включительно, зарезервированы для приватного использования [RFC5226].

6. Благодарности

Авторы хотят выразить благодарность Alfred Hoenes и Ted Hardie за их предложения по улучшению данного документа.

7. Литература

7.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, November 2007.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC6066] Eastlake 3rd, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, January 2011.

7.2. Дополнительная литература

[RFC5081] Mavrogiannopoulos, N., "Using OpenPGP Keys for Transport Layer Security (TLS) Authentication", RFC 5081, November 2007.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

Приложение A. Отличия от RFC 5081

Этот документ включает существенные изменения сообщений TLS «Server Certificate» и «Client Certificate», что делает реализации данного протокола несовместимыми с реализациями [RFC5081]. Эти изменения требуют явной маркировки идентификаторов субключей, используемых для аутентификации TLS, в процедуре согласования. Это было сделано для того, чтобы не вносить ограничений на содержимое сертификатов OpenPGP, которые могут применяться в данном протоколе.

[RFC5081] требует, чтобы ключ или субключ OpenPGP маркировался флагом аутентификации; поэтому засвидетельствование может завершаться отказом, если этот флаг установить для нескольких субключей. Данный протокол снимает это ограничение.

Адреса авторов

Nikos Mavrogiannopoulos
ESAT/COSIC Katholieke Universiteit Leuven
Kasteelpark Arenberg 10, bus 2446
Leuven-Heverlee, B-3001
Belgium
EMail: nikos.mavrogiannopoulos@esat.kuleuven.be

Daniel Kahn Gillmor
Independent
119 Herkimer St.
Brooklyn, NY 11216-2801
US
EMail: dkg@fifthhorseman.net

Перевод на русский язык
Николай Малых
nmalykh@gmail.com