Internet Engineering Task Force (IETF)
Request for Comments: 8002
Obsoletes: 6253
Updates: 7401
Category: Standards Track
ISSN: 2070-1721

T. Heer
Albstadt-Sigmaringen University
S. Varjonen
University of Helsinki

October 2016

Host Identity Protocol Certificates

Сертификаты протокола идентификации хостов (HIP)

Аннотация

Параметр Certificate (CERT) является контейнером для цифровых сертификатов и служит для передачи этих сертификатов в пакетах управления протокола идентификации хостов (Host Identity Protocol или HIP). Документ задаёт параметр сертификата и сигнализацию ошибок в случае отказа при проверке сертификата. Кроме того, документ задаёт представление тегов отождествления хоста (Host Identity Tag или HIT) в X.509 версии 3 (v3).

Конкретные варианты применения сертификатов, включая способы получения и запроса, а также действия при подтверждении или отказе в процессе проверки сертификата зависят от сценария использования. Поэтому определения таких аспектов оставлены для документов об использовании параметра CERT.

Документ обновляет RFC 7401 и отменяет RFC 6253.

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/rfc8002.

Оглавление

1. Введение

Цифровые сертификаты связывают фрагменты информации с открытым ключом с помощью цифровой подписи и, таким образом, позволяют позволяют владельцу секретного ключа создавать криптографически проверяемые заявления. Протокол идентификации хоста (HIP) [RFC7401] определяет новое криптографическое пространство имён на основе асимметричной криптографии. Отождествление каждого хоста выводится из открытого ключа, позволяя хостам использовать цифровые подписи данных и выдавать сертификаты по своему секретному ключу. Этот документ задаёт параметр CERT, служащий для передачи цифровых сертификатов в HIP. Параметр подставляется вместо заменителя (placeholder), заданного в параграфе 5.2 [RFC7401] и, таким образом, обновляет [RFC7401].

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

1.1. Уровни требований

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. Параметр CERT

Параметр CERT является контейнером для некоторых типов цифровых сертификатов, но не задаёт семантики сертификата. Однако параметр определяет дополнительные параметры, помогающие хостам HIP передавать семантически сгруппированные параметры CERT более систематизированным способом. Конкретное использование параметра CERT в разных сценариях не рассматривается в этом документе и будет определяться в документах, посвящённых вариантам применения CERT.

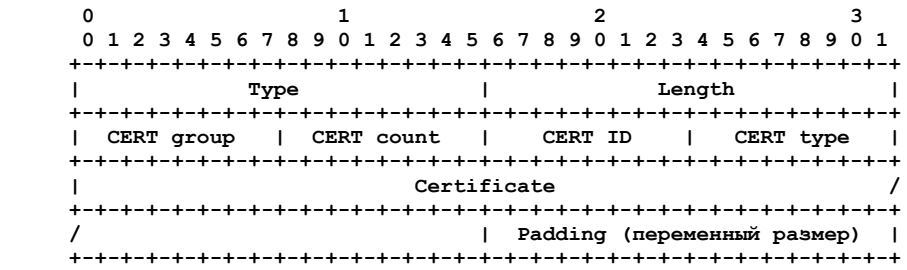
При наличии параметра CERT он учитывается и защищается полем HIP SIGNATURE, не являясь критическим.

Параметр CERT можно использовать во всех пакетах HIP. Однако его включение в первый пакет инициатора (I1) **не рекомендуется**, поскольку это может увеличить время обработки I1, что может создавать проблемы при обработке «шквалов» I1. Каждый пакет управления HIP **может** включать несколько параметров CERT со своими сертификатами. Эти параметры **могут** быть связанными или несвязанными. Связанные сертификаты поддерживаются в группах CERT. Группа CERT задаёт набор связанных параметров CERT, которые **следует** интерпретировать в определённом порядке (например, для цепочек сертификатов). Несгруппированные сертификаты показывают уникальное поле группы CERT и для них устанавливается значение счётчика CERT 1. Параметры CERT с одним номером группы в поле CERT group показывают логическую группировку. Поле CERT указывает число параметров CERT в группе.

Параметры CERT из одной группы CERT **могут** передаваться в нескольких последовательных пакетах управления HIP. Это указывается значением CERT count, превышающим число параметров CERT с соответствующим полем CERT group в пакетах управления HIP. Параметры CERT должны упорядочиваться в порядке возрастания номеров в пакете управления HIP, согласно полю CERT group. Группа CERT **может** включать множество пакетов лишь в том случае, когда она не помещается в пакет. В пакет HIP **недопустимо** включать более одной неполной группы CERT, которая будет продолжаться в следующем пакете управления HIP.

CERT ID служит порядковым номером для идентификации сертификатов в группе CERT. Значения CERT ID **должны** находиться в интервале от 1 до CERT count.

Пространства имён CERT group и CERT ID поддерживаются локально каждым хостом, передающим параметры CERT в пакетах управления HIP.



Type
768

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

CERT group
Group ID для группы связанных параметров CERT.

CERT count
Общее число передаваемых сертификатов (возможно в нескольких последовательных пакетах управления HIP).

CERT ID
Порядковый номер сертификата.

CERT Type
Тип сертификата.

Padding
Заполнение до размера TLV, кратного 8 байтам. Байты заполнения **должны** иметь значение 0 при передаче, а получателю **не следует** проверять их.

Сертификаты **должны** использовать алгоритмы, указанные в [RFC7401], для подписи и хэширования. Поддерживаемые алгоритмы указаны в таблице.

Формат CERT	*Тип*
Резерв	0
X.509 v3	1
Устарел	2
Hash и URL из X.509 v3	3
Устарел	4
LDAP URL из X.509 v3	5
Устарел	6
Отличительное имя (Distinguished Name) из X.509 v3	7
Устарел	8

В следующем параграфе рассмотрено использование HIT в X.509 v3. Сертификаты X.509 v3 и процедуры обработки заданы в [RFC5280]. Формат при передаче X.509 v3 задают правила DER (Distinguished Encoding Rules) из [X.690].

Применяется кодирование «Хэш и URL» (3), заданное в параграфе 3.6 [RFC7296]. Это кодирование обеспечивает меньший размер пакетов управления HIP, нежели при включении сертификатов, но требует от получателя преобразовать URL или сравнить хэш-значение с локальным кэшем.

Кодирование LDAP URL (5) применяется в соответствии с [RFC4516]. Это кодирование снижает размер пакетов управления HIP, но требует от получателя извлечения сертификата или сравнения URL с локальным кэшем.

Кодирование (DN) (7) представляется отличительным именем (DN) субъекта сертификата, как указано в [RFC4514]. Это кодирование снижает размер пакетов управления HIP, но требует от получателя извлечь сертификат или сравнить DN с локальным кэшем.

3. Объект сертификата X.509 v3 и отождествления хостов

При необходимости теги HIT могут представлять эмитента (issuer) и/или субъект в сертификате X.509 v3. Теги HIT представляются в форме адресов IPv6, как указано в [RFC7343]. При использовании идентификатора хоста (HI) для подписывания сертификата **следует** включать соответствующий тег HIT в расширение IAN (Issuer Alternative Name - дополнительное имя эмитента), используя форму GeneralName для iPAddress, как указано в [RFC5280]. Когда сертификат выпущен для хоста HIP, идентифицируемого HIT и HI, **следует** включать тег HIT в расширение SAN (Subject Alternative Name - дополнительное имя субъекта), используя форму GeneralName для iPAddress, а полный идентификатор HI представляется как информация об открытом ключе субъекта в соответствии с [RFC5280].

Ниже даны примеры представления HIT как эмитента и субъекта в расширениях дополнительных имён X.509 v3.

```
Формат расширений X509v3:
        X509v3 Issuer Alternative Name:
                IP Address:hit-of-issuer
        X509v3 Subject Alternative Name:
                IP Address:hit-of-subject

Пример расширений X509v3:
        X509v3 Issuer Alternative Name:
                IP Address:2001:24:6cf:fae7:bb79:bf78:7d64:c056
        X509v3 Subject Alternative Name:
                IP Address:2001:2c:5a14:26de:a07c:385b:de35:60e3
```

В Приложении A приведён пример полного сертификата X.509 v3 с содержимым HIP.

В качестве другого примера рассмотрим среду PKI (Public Key Infrastructure), где партнёры имеют сертификаты, привязанные к (потенциально разным) управляемым цепочкам доверия. В этом случае выпускаемые для хостов HIP сертификаты подписываются промежуточными удостоверяющими центрами (Certification Authority или CA) вплоть до корневого CA. Управляемая среда PKI в этом случае не знает о HIP и не настраивается на расчёт HIT и включение тегов в сертификаты.

Когда взаимодействие HIP организовано, хостам HIP нужно передавать не только свой сертификат отождествления (или указатель на него), но и сертификаты промежуточных CA (или указатели на них) вплоть до корневого CA или сертификат доверенного для удалённого партнёра CA. Эту цепочку сертификатов **следует** передавать в группе CERT, как указано в разделе 2. Партнёры HIP проверяют сертификаты друг друга и рассчитывают HIT на основе открытых ключей в сертификатах.

4. Отзыв сертификатов

Отзыв сертификатов X.509 v3 обрабатывается в соответствии с разделом 5 в [RFC5280] с 2 исключениями. Во-первых, любой порядковый номер сертификата HIP в списке отзыва (Certificate Revocation List или CRL) считается недействительным независимо от кода причины. Во-вторых, certificateHold не поддерживается.

5. Сигналы об ошибках

Если инициатор не передаёт всех запрошенных ответчиком (Responder) сертификатов, ответчик может реагировать на это (например, разорвать соединение). Ответчик **может** сигнализировать это инициатору отправкой сообщения HIP NOTIFY с параметром NOTIFICATION и типом ошибки CREDENTIALS_REQUIRED.

Если проверка сертификата привела к отказу, проверяющий **может** сообщить об этом поставщику сертификата сообщением HIP NOTIFY с параметром NOTIFICATION и типом ошибки INVALID_CERTIFICATE.

CREDENTIALS_REQUIRED 48

Ответчик не хочет создавать ассоциацию, поскольку инициатор не передал требуемых свидетельств (credential).

INVALID_CERTIFICATE 50

Передаётся при отказе в процессе проверки сертификата. Данные уведомления **могут** включать CERT group и октет CERT ID (в указанном порядке) из параметра CERT, связанного с отказом.

6. Взаимодействие с IANA

Документ определяет параметр CERT для протокола HIP [RFC7401] с номером 768, заданным в [RFC7401]. Параметр CERT включает поле с 8-битовым целым числом без знака для разных типов сертификатов, для которых в IANA создан и поддерживается субреестр HIP Certificate Types в реестре Host Identity Protocol (HIP) Parameters. Значения для реестра HIP Certificate Types даны в разделе 2. Новые значения выделяются из свободного пространства по процедуре IETF Review.

В разделе 5 этого документа заданы два значения для субреестра NOTIFY Message Types в реестре Host Identity Protocol (HIP) Parameters". Поскольку этот документ отменяет [RFC6253], ссылки на [RFC6253] в реестрах IANA заменяются ссылками на этот документ. Документ меняет содержимое реестра HIP Certificate Types в разделе 2.

- Ссылки на [RFC6253] заменены ссылками на этот документ.
- Отменены типы сертификатов с номерами 2, 4, 6, 8 для Simple Public Key Infrastructure (SPKI).

7. Вопросы безопасности

Группировка сертификатов позволяет передавать их в нескольких последовательных пакетах. Это может открыть возможность для атак, поскольку фрагментация уровня IP позволяет, например, передавать фрагменты с нарушением порядка и пропускать некоторые фрагменты для задержки или остановки обработки пакетов на стороне жертвы с целью расхода ресурсов (например, CPU или памяти). Поэтому хостам **следует** реализовать механизмы для отбрасывания группы сертификатов при ограниченном пространстве состояний.

Хотя параметр CERT можно передавать в пакетах I1, это **не рекомендуется**, поскольку может увеличивать время обработки I1, что может создать проблемы при обработке «шквала» пакетов I1. Кроме того, инициаторам следует учитывать, что ответчик может отбросить параметр CERT в пакете I1 без обработки этого параметра.

Проверка URL и записей LDAP может открыть возможность для атак на службу (denial-of-service или DoS), вынуждающих целевой хост выполнять ненужную работу.

Вопросы безопасности X.509 v3 рассмотрены в [RFC5280].

8. Отличия от RFC 6253

В этом разделе приведена сводка технических отличий от [RFC6253]. Раздел является информационным и предназначен для оказания помощи разработчикам, использовавшим предыдущую версию протокола. Если текст этого раздела противоречит другому тексту данной спецификации, нормативным следует считать текст вне этого раздела.

Этот документ исключает поддержку сертификатов SPKI.

9. Литература

9.1. 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>.

[RFC4514] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names", RFC 4514, DOI 10.17487/RFC4514, June 2006, <http://www.rfc-editor.org/info/rfc4514>.

[RFC4516] Smith, M., Ed. and T. Howes, "Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator", RFC 4516, DOI 10.17487/RFC4516, June 2006, <http://www.rfc-editor.org/info/rfc4516>.

[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, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <http://www.rfc-editor.org/info/rfc7296>.

[RFC7343] Laganier, J. and F. Dupont, "An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers Version 2 (ORCHIDv2)", RFC 7343, DOI 10.17487/RFC7343, September 2014, <http://www.rfc-editor.org/info/rfc7343>.

[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>.

[X.690] ITU-T, , "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690 | ISO/IEC 8825-1, August 2015.

9.2. Дополнительная литература

[RFC6253] Heer, T. and S. Varjonen, "Host Identity Protocol Certificates", RFC 6253, DOI 10.17487/RFC6253, May 2011, <http://www.rfc-editor.org/info/rfc6253>.

Приложение A. Пример сертификата X.509 v3

В этом приложении показан сертификат X.509 v3 с закодированными HIT.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 12705268244493839545 (0xb0522e27291b2cb9)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=Example, DC=com, CN=Example issuing host
        Validity
            Not Before: Feb 25 11:28:29 2016 GMT
            Not After : Feb 24 11:28:29 2017 GMT
        Subject: DC=Example, DC=com, CN=Example issuing host
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c9:b0:85:94:af:1f:3a:77:39:c9:d5:81:a5:ee:
                    d2:b5:6b:72:91:5d:22:2c:1e:59:e5:06:29:bd:a2:
                    19:f6:ac:ca:eb:f7:88:d8:54:55:41:01:58:d8:87:
                    64:d8:c8:cf:6e:c2:38:81:22:1a:ae:e9:a6:80:22:
                    03:ee:f3:1b:7e:68:11:e3:f4:7b:98:33:28:bf:40:
                    ec:4f:19:e8:10:8a:8b:07:60:f7:9f:e4:82:f8:a7:
                    58:04:3d:42:07:c8:34:ca:99:6d:11:eb:73:c1:d9:
                    96:93:55:e5:c7:ed:80:4f:8a:f2:1a:6f:83:c8:15:
```

```
                    a4:8f:b8:6a:fe:f3:4f:49:1a:5c:1f:89:bb:30:e6:
                    98:bc:ce:a3:a2:37:85:b1:79:1c:26:e6:44:0c:b9:
                    3e:d8:37:81:46:f4:02:25:46:a2:ea:da:25:5c:46:
                    a2:a3:c5:58:80:53:1f:c5:e5:11:a0:da:d8:f2:ad:
                    d6:98:d4:ce:55:35:cc:0b:d3:5b:09:48:ef:57:65:
                    80:cb:65:79:fd:cb:4d:5b:b3:8d:1a:ff:2a:58:3e:
                    96:65:10:3e:04:81:78:2b:d5:ca:89:78:ea:28:5c:
                    bc:02:4a:54:cd:aa:a9:99:8d:d6:39:e9:5e:a9:73:
                    1a:5d:93:55:39:9b:72:1a:c2:a0:1f:e3:4c:b0:41:
                    98:97
                Exponent: 65537 (0x10001)
            X509v3 extensions:
                X509v3 Subject Alternative Name:
                    IP Address:2001:27:DCFC:CB8:F885:D53F:4E63:48B7
                X509v3 Issuer Alternative Name:
                    IP Address:2001:2D:F878:64C1:67E3:9716:88BD:68E4
        Signature Algorithm: sha256WithRSAEncryption
             6d:e6:a9:a6:30:c4:ab:3e:86:39:1e:de:76:4d:4e:a4:2d:63:
             4d:bb:41:bf:d3:0c:66:13:8b:4d:b2:50:59:36:fc:ae:42:9e:
             c8:a0:41:1a:1c:94:56:05:28:82:34:4e:63:75:87:31:25:67:
             36:a6:1a:0f:b8:f7:db:03:e7:dd:a6:9a:26:c4:68:e2:cf:59:
             54:e6:ee:cc:a7:ce:fb:56:bf:31:60:f4:cb:e7:f0:0e:50:f8:
             b7:c5:3c:1a:de:74:d0:aa:83:e5:15:25:b1:bf:be:a4:7f:af:
             0a:de:08:09:0e:13:1d:2a:3b:1a:99:d9:af:10:fc:08:92:5f:
             d8:d0:10:d6:b9:0c:86:da:85:3b:44:b5:97:90:10:02:4f:5a:
             1f:ae:07:30:6b:f5:e6:12:93:72:e2:10:c9:8e:2c:00:8b:d6:
             f0:05:c3:ff:91:24:69:6d:5b:5a:0c:40:28:01:f2:5b:45:b8:
             9b:ae:9e:73:e9:dd:83:e0:85:d7:ad:6c:b1:81:ac:a0:30:37:
             9d:60:bd:92:3b:d2:a1:21:87:8b:c4:d9:5a:5c:21:56:3e:02:
             7e:f3:6f:a5:de:40:75:80:f5:41:68:5c:b2:61:fb:1d:9a:a5:
             97:a8:d4:a9:82:45:86:79:3c:63:76:3d:fd:86:a0:f8:14:84:
             55:c1:8c:fa
```

```
-----BEGIN CERTIFICATE-----
MIIDWTCCAkGgAwIBAgIJALBSLicpGyy5MA0GCSqGSIb3DQEBCwUAME0xFzAVBgoJ
kiaJk/IsZAEZFgdFeGFtcGxlMRMwEQYKCZImiZPyLGQBGRYDY29tMR0wGwYDVQQD
ExRFeGFtcGxlIGlzc3VpbmcgaG9zdDAeFw0xNjAyMjUxMTI4MjlaFw0xNzAyMjQx
MTI4MjlaME0xFzAVBgoJkiaJk/IsZAEZFgdFeGFtcGxlMRMwEQYKCZImiZPyLGQB
GRYDY29tMR0wGwYDVQQDExRFeGFtcGxlIGlzc3VpbmcgaG9zdDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMmwhZSvHzp3OcnVgaXu0rVrcpFdIiweWeUG
Kb2iGfasyuv3iNhUVUEBWNiHZNjIz27COIEiGq7ppoAiA+7zG35oEeP0e5gzKL9A
7E8Z6BCKiwdg95/kgvinWAQ9QgfINMqZbRHrc8HZlpNV5cftgE+K8hpvg8gVpI+4
av7zT0kaXB+JuzDmmLzOo6I3hbF5HCbmRAy5Ptg3gUb0AiVGouraJVxGoqPFWIBT
H8XlEaDa2PKt1pjUzlU1zAvTWwlI71dlgMtlef3LTVuzjRr/Klg+lmUQPgSBeCvV
yol46ihcvAJKVM2qqZmN1jnpXqlzGl2TVTmbchrCoB/jTLBBmJcCAwEAAaM8MDow
GwYDVR0RBBQwEocQIAEAJ9z8DLj4hdU/TmNItzAbBgNVHRIEFDAShxAgAQAt+Hhk
wWfjlxaIvWjkMA0GCSqGSIb3DQEBCwUAA4IBAQBt5qmmMMSrPoY5Ht52TU6kLWNN
u0G/0wxmE4tNslBZNvyuQp7IoEEaHJRWBSiCNE5jdYcxJWc2phoPuPfbA+fdppom
xGjiz1lU5u7Mp877Vr8xYPTL5/AOUPi3xTwa3nTQqoPlFSWxv76kf68K3ggJDhMd
KjsamdmvEPwIkl/Y0BDWuQyG2oU7RLWXkBACT1ofrgcwa/XmEpNy4hDJjiwAi9bw
BcP/kSRpbVtaDEAoAfJbRbibrp5z6d2D4IXXrWyxgaygMDedYL2SO9KhIYeLxNla
XCFWPgJ+82+l3kB1gPVBaFyyYfsdmqWXqNSpgkWGeTxjdj39hqD4FIRVwYz6
-----END CERTIFICATE-----
```

Благодарности

Авторы благодарны A. Keranen, D. Mattes, M. Komu, T. Henderson за плодотворное обсуждение. D. Mattes внёс большой вклад в описание случая работы без поддержки HIP в разделе 3.

Адреса авторов

Tobias Heer
Albstadt-Sigmaringen University
Poststr. 6
72458 Albstadt
Germany
Email: heer@hs-albsig.de

Samu Varjonen
University of Helsinki
Gustaf Haellstroemin katu 2b
00560 Helsinki
Finland
Email: samu.varjonen@helsinki.fi

Перевод на русский язык
Николай Малых
nmalykh@protokols.ru