Internet Engineering Task Force (IETF)
Request for Comments: 8447
Updates: 3749, 5077, 4680, 5246, 5705,
5878, 6520, 7301
Category: Standards Track
ISSN: 2070-1721

J. Salowey
Tableau Software
S. Turner
sn3rd

August 2018

IANA Registry Updates for TLS and DTLS

Обновление реестров IANA для TLS и DTLS

Аннотация

Этот документ описывает многочисленные изменения в реестрах IANA для TLS и DTLS от примечаний в реестрах до изменения политики регистрации. Эти изменения вызваны в основном обзором реестров рабочей группой в процессе разработки спецификации TLS 1.3.

Этот документ обновляет RFC 3749, RFC 5077, RFC 4680, RFC 5246, RFC 5705, RFC 5878, RFC 6520, RFC 7301.

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 https://www.rfc-editor.org/info/rfc8447.

Оглавление

1. Введение....1
2. Уровни требований....2
3. Добавление TLS в имена реестров....2
4. Соответствие RFC 8126....2
5. Добавление столбца Recommended....2
6. Расширение TLS Session Ticket....2
7. Значения TLS ExtensionType....2
8. Реестр TLS Cipher Suites....3
9. Поддерживаемые TLS группы....4
10. Идентификаторы TLS ClientCertificateType....5
11. Новый тип сообщений Session Ticket TLS Handshake....5
12. Реестр TLS Exporter Labels....5
13. Добавление отсутствовавшего элемента в реестр TLS Alerts....6
14. Типы сертификатов TLS....6
15. «Осиротевшие» реестры....6
16. Дополнительные замечания....7
17. Назначенные эксперты....7
18. Вопросы безопасности....7
19. Взаимодействие с IANA....7
20. Литература....8
20.1. Нормативные документы....8
20.2. Дополнительная литература....8
Адреса авторов....8

1. Введение

В соответствии с этим документом агентство IANA внесло множество изменений в реестры IANA, связанные с протоколами защиты транспортного уровня TLS (Transport Layer Security) и DTLS (Datagram Transport Layer Security). Эти изменения почти полностью вызваны разработкой спецификации TLS 1.3 [RFC8446].

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

Внесённые этим документом изменения варьируются от простых, например, добавления примечаний, до комплексных, таких как смена политики регистрации. Вместо перечисления и обоснования этих изменений во введении, обоснования приведены в отдельных параграфах.

Этот документ не меняет правила регистрации для реестров TLS Alerts [RFC8446], TLS ContentType [RFC8446], TLS HandshakeType [RFC8446], TLS Certificate Status Types [RFC6961], поскольку имеющиеся правила (Standards Action для трёх первых и IETF Review для последнего) подходят для этих однобайтовых кодов по причине их немногочисленности.

2. 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 BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

3. Добавление TLS в имена реестров

Для согласованности реестров TLS агентство IANA добавило префикс TLS к именам перечисленных ниже реестров.

- Application-Layer Protocol Negotiation (ALPN) Protocol IDs [RFC7301].
- ExtensionType Values.
- Heartbeat Message Types [RFC6520].
- Heartbeat Modes [RFC6520].

Агентство IANA обновило ссылки в этих реестрах с указанием данного документа. Далее в этом документе реестры именуются с префиксом TLS.

4. Соответствие RFC 8126

Многие из связанных с TLS реестров IANA используют процедуру регистрации IETF Consensus, которая была заменена процедурой IETF Review в [RFC8126]. С учётом этого агентство IANA указало процедуру IETF Review в перечисленных ниже реестрах.

- TLS Authorization Data Formats [RFC4680].
- TLS Supplemental Data Formats (SupplementalDataType) [RFC5878]

Это не универсальная замена, поскольку в некоторые реестры с процедурой IETF Consensus внесены изменения данным документом, [RFC8446] или [RFC8422].

Агентство IANA обновило ссылки в двух указанных реестрах, добавив ссылку на этот документ.

5. Добавление столбца Recommended

В соответствии с этим документом добавлен столбец Recommended (Рекомендуется) во многие реестры TLS для указания параметров, поддержка которых обычно рекомендуется в реализации. Добавление параметра Recommended (т. е. Y) в реестр или смена статуса Recommended выполняется по процедуре Standards Action. Не для всех параметров, заданных в документах Standards Track требуется маркировка Recommended.

Если элемент не помечен как рекомендуемый (т. е. N), это не обязательно указывает его изъян, этого говорит скорее о том, что элемент не прошёл процедуру согласования (IETF consensus), имеет ограниченную применимость или предназначен для особых случаев применения.

6. Расширение TLS Session Ticket

Номенклатура записей реестра TLS ExtensionType Values соответствует имени поля языка представления за исключением записи 35. Для согласованного представления записей в реестре агентство IANA:

- переименовало запись 35 в session_ticket (вместо SessionTicket TLS из [RFC5077]);
- добавило ссылку на этот документ в столбец Reference записи 35.

7. Значения TLS ExtensionType

Опыт показывает, что процедура IETF Review для расширений TLS слишком строга. Рабочая группа приняла решение о замене процедуры на Specification Required [RFC8126] с сохранением небольшой части кодов для приватного использования. В результате реестр TLS ExtensionType Values был обновлён IANA, как указано ниже.

- Изменена процедура регистрации.

  Значения с первым байтом от 0 до 254 (десятичное) выделяются по процедуре Specification Required [RFC8126]. Значения с первым байтом 255 (десятичное) выделяются для приватного использования (Private Use) [RFC8126].

- Обновленный столбец Reference указывает также этот документ.

Назначение экспертов дополнительно описано в разделе 17.

Несмотря на желание «смягчить» процедуру регистрации расширений TLS, полезно указать в реестре IANA расширения, поддержку которых рекомендует рабочая группа (WG). Поэтому агентство IANA обновило реестр TLS ExtensionType Values, как показано ниже.

- Добавлен столбец Recommended (Рекомендуется), как показано в таблице ниже. При создании таблицы Для всех RFC со статусом Standards Track было установлено значение Y (рекомендуется), для остальных - N (не рекомендуется). Значение N в столбце Recommended устанавливается, если явно не запрошено иное, а установка Y выполняется по процедуре Standards Action [RFC8126]. Для смены Y на N **требуется** процедура IESG Approval.

Расширение	***Рекомендуется***
server_name	Y
max_fragment_length	N
client_certificate_url	Y
trusted_ca_keys	Y
truncated_hmac	Y
status_request	Y
user_mapping	Y
client_authz	N
server_authz	N
cert_type	N
supported_groups	Y
ec_point_formats	Y
srp	N
signature_algorithms	Y
use_srtp	Y
heartbeat	Y
application_layer_protocol_negotiation	Y
status_request_v2	Y
signed_certificate_timestamp	N
client_certificate_type	Y
server_certificate_type	Y
padding	Y
encrypt_then_mac	Y
extended_master_secret	Y
cached_info	Y
session_ticket	Y
renegotiation_info	Y

Агентство IANA добавило в реестр указанные ниже примечания.

> Примечание. Роль назначенного эксперта описана в RFC 8447. Назначенный эксперт [RFC8126] обеспечивает публичную доступность спецификации. Для этого достаточно иметь документ Internet-Draft (который отправлен, но не опубликован в RFC) или документ оного органа стандартизации, отраслевого консорциума, университета и т. п. Эксперт может представить более глубокую рецензию, но одобрение эксперта не следует рассматривать как поддержку данного расширения.
>
> Примечание. Как указано в [RFC8126], назначения из пространства Private Use обычно бесполезны для широкого взаимодействия (совместимости). Использующие значения из этого диапазона принимают на себя ответственность за предотвращение конфликтов значения (в предполагаемой области применения). Для более широких экспериментов доступны временно выделяемые значения.
>
> Примечание. Если элемент не указан как Recommended, это не обязательно говорит о его изъянах, а указывает лишь, что элемент не прошёл процедуру согласования IETF, имеет ограниченную применимость или предназначен для использования в особых (конкретных) случаях.

Расширения, добавленные [RFC8446], не включены в таблицу и опущено также расширение token_binding, поскольку в [TOKBIND] для него указано значение колонки Recommended.

[RFC8446] использует реестр TLS ExtensionType Values, созданный [RFC4366]. Ниже приведён текст из [RFC8446] для согласования этих спецификаций.

- Агентство IANA обновило реестр, добавив расширения key_share, pre_shared_key, psk_key_exchange_modes, early_data, cookie, supported_versions, certificate_authorities, oid_filters, post_handshake_auth и signature_algorithms_cert со значениями, заданными у этом документе и Recommended = Y.
- Агентство IANA обновило реестр, включив колонку TLS 1.3, где указываются сообщения, в которых может присутствовать расширение. Эта колонка заполнена значениями в соответствии с таблицей из параграфа 4.2, а не указанные в таблице расширения помечены символом «-», указывающим, что они не применяются в TLS 1.3.

8. Реестр TLS Cipher Suites

Опыт показывает, что процедура IETF Consensus для TLS Cipher Suites слишком строга. Рабочая группа приняла решение о замене процедуры на Specification Required [RFC8126] с сохранением небольшой части кодов для приватного использования. В результате реестр TLS Cipher Suites был обновлён IANA, как указано ниже.

> Значения с первым байтом от 0 до 254 (десятичное) выделяются по процедуре Specification Required [RFC8126]. Значения с первым байтом 255 (десятичное) выделяются для приватного использования (Private Use) [RFC8126].

Назначение экспертов дополнительно описано в разделе 17.

Реестр TLS Cipher Suites был существенно расширен и продолжает расширяться. Чтобы реестр был лучше понятен тем, кто не связан тесно с TLS, агентство IANA внесло в реестр TLS Cipher Suites указанное ниже изменение.

- Добавлен столбец Recommended (Рекомендуется). Шифрам, указанным в двух следующих таблицах для этого столбца задано значение Y (рекомендуется), для остальных - N (не рекомендуется). Значение N в столбце

Recommended устанавливается, если явно не запрошено иное, а установка Y выполняется по процедуре Standards Action [RFC8126]. Для смены Y на N требуется процедура IESG Approval.

В следующей таблице приведены шифронаборы из Standards Track с аутентификацией на сервере (возможно и у клиента), доступные в настоящее время для TLS 1.2.

Имя шифронабора	*Значение*
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	{0x00,0x9E}
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	{0x00,0x9F}
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	{0xC0,0x2B}
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	{0xC0,0x2C}
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	{0xC0,0x2F}
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	{0xC0,0x30}
TLS_DHE_RSA_WITH_AES_128_CCM	{0xC0,0x9E}
TLS_DHE_RSA_WITH_AES_256_CCM	{0xC0,0x9F}
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	{0xCC,0xA8}
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	{0xCC,0xA9}
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	{0xCC,0xAA}

В следующей таблице приведены шифронаборы из Standards Track с с эфемерными, заранее распространяемыми (pre-shared) ключами, доступные в настоящее время для TLS 1.2.

Имя шифронабора	*Значение*
TLS_DHE_PSK_WITH_AES_128_GCM_SHA256	{0x00,0xAA}
TLS_DHE_PSK_WITH_AES_256_GCM_SHA384	{0x00,0xAB}
TLS_DHE_PSK_WITH_AES_128_CCM	{0xC0,0xA6}
TLS_DHE_PSK_WITH_AES_256_CCM	{0xC0,0xA7}
TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256	{0xD0,0x01}
TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384	{0xD0,0x02}
TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256	{0xD0,0x05}
TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256	{0xCC,0xAC}
TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256	{0xCC,0xAD}

Шифронаборы TLS 1.3, заданные в [RFC8446], не указаны в таблицах. Этот документ задаёт для них статус Recommended.

Опыт показал, что некоторые клиенты считают реестр IANA контрольным списком для оценки полноты реализации, а некоторые разработчики слепо реализуют шифры. Такой подход является ошибочным, поэтому агентство IANA добавило в реестр приведённое ниже предупреждение.

> Предупреждение. Криптографические алгоритмы и параметры могут с течением времени взломаны или сочтены слабыми. Слепая реализация указанных в списке шифров не рекомендуется. Разработчикам и пользователям необходимо проверять наличие и статус алгоритмов в списке для обеспечения требуемого уровня защиты.

Агентство IANA добавило приведённое ниже примечание, чтобы указать занимающимся реестрами IANA, что в TLS 1.3 [RFC8446] используются те же реестры, но шифры определяются иначе.

> Примечание. Хотя в TLS 1.3 применяется то же пространство шифронаборов, что и в предшествующих версиях TLS, шифры в TLS 1.3 определены с указанием лишь симметричных шифров и хэш-функций и не могут применяться для TLS 1.2. Точно так же шифры TLS 1.2 и ниже не пригодны для TLS 1.3.

Агентство IANA добавило приведённые ниже примечания для документирования правил заполнения столбца Recommended.

> Примечание. Шифры CCM_8 не помечены как Recommended. Эти шифры имеют сильно усечённый тег аутентификации, задающий уровень защиты, который может не подходить для сред общего назначения.

> Примечание. Если элемент не помечен как Recommended, это не обязательно говорит о его изъянах, а указывает лишь, что элемент не прошёл процедуру согласования IETF, имеет ограниченную применимость или предназначен для использования в особых (конкретных) случаях.

Агентство IANA добавило приведённые ниже примечания с дополнительной информацией.

> Примечание. Роль назначенного эксперта описана в RFC 8447. Назначенный эксперт [RFC8126] обеспечивает публичную доступность спецификации. Для этого достаточно иметь документ Internet-Draft (который отправлен, но не опубликован в RFC) или документ оного органа стандартизации, отраслевого консорциума, университета и т. п. Эксперт может представить более глубокую рецензию, но одобрение эксперта не следует рассматривать как поддержку данного шифра.

> Примечание. Как указано в [RFC8126], назначения из пространства Private Use обычно бесполезны для широкого взаимодействия (совместимости). Использующие значения из этого диапазона принимают на себя ответственность за предотвращение конфликтов значения (в предполагаемой области применения). Для более широких экспериментов доступны временно выделяемые значения.

Агентство IANA обновило ссылки в этом реестре, добавив данный документ.

9. Поддерживаемые TLS группы

Как и шифронаборы, поддерживаемые группы со временем множились и некоторые люди рассматривают реестр как мерило соответствия реализаций. Поэтому агентство IANA добавило столбец Recommended со значением Y для групп secp256r1, secp384r1, x25519, x448, указав для остальных значение N. Группы Y взяты из RFC со статусом Standards Track, а [RFC8422] повышает статус secp256r1 и secp384r1 до Standards Track. Не все группы из [RFC8422], относящиеся к Standards Track, получили статус Y, эти группы применимы к TLS 1.3 [RFC8446] и прежним версиям TLS. Значение N в столбце Recommended устанавливается, если явно не запрошено иное, а установка Y выполняется по процедуре Standards Action [RFC8126]. Для смены Y на N **требуется** процедура IESG Approval.

Агентство IANA добавило в реестр приведённые ниже примечания.

> Примечание. Если элемент не помечен как Recommended, это не обязательно говорит о его изъянах, а указывает лишь, что элемент не прошёл процедуру согласования IETF, имеет ограниченную применимость или предназначен для использования в особых (конкретных) случаях.
>
> Примечание. Роль назначенного эксперта описана в RFC 8447. Назначенный эксперт [RFC8126] обеспечивает публичную доступность спецификации. Для этого достаточно иметь документ Internet-Draft (который отправлен, но не опубликован в RFC) или документ оного органа стандартизации, отраслевого консорциума, университета и т. п. Эксперт может представить более глубокую рецензию, но одобрение эксперта не следует рассматривать как продвижение данной поддерживаемой группы.

Опыт показал, что некоторые клиенты считают реестр IANA контрольным списком для оценки полноты реализации, а некоторые разработчики слепо реализуют поддерживаемые группы. Такой подход является ошибочным, поэтому агентство IANA добавило в реестр приведённое ниже предупреждение.

> Предупреждение. Криптографические алгоритмы и параметры могут с течением времени взломаны или сочтены слабыми. Слепая реализация указанных в списке поддерживаемых групп не рекомендуется. Разработчикам и пользователям необходимо проверять наличие и статус алгоритмов в списке для обеспечения требуемого уровня защиты.

Агентство IANA обновило ссылки в этом реестре, добавив данный документ.

Значение 0 (0x0000) указано как резервное.

10. Идентификаторы TLS ClientCertificateType

Опыт показывает, что процедура IETF Consensus для TLS ClientCertificateType Identifiers слишком строга. Рабочая группа приняла решение о замене процедуры на Specification Required [RFC8126] с сохранением некоторой части кодов Standards Track и небольшой части для приватного использования. В результате реестр TLS ClientCertificateType Identifiers был обновлён IANA, как указано ниже.

> Значения от 0 до 63 распределяются по процедуре Standards Action.
>
> Значения от 64 до 223 распределяются по процедуре Specification Required [RFC8126].
>
> Значения от 224 до 255 резервируются для приватного использования (Private Use).

Назначение экспертов дополнительно описано в разделе 17.

Агентство IANA добавило приведённые ниже примечания с дополнительной информацией.

> Примечание. Роль назначенного эксперта описана в RFC 8447. Назначенный эксперт [RFC8126] обеспечивает публичную доступность спецификации. Для этого достаточно иметь документ Internet-Draft (который отправлен, но не опубликован в RFC) или документ оного органа стандартизации, отраслевого консорциума, университета и т. п. Эксперт может представить более глубокую рецензию, но одобрение эксперта не следует рассматривать как поддержку данного идентификатора.
>
> Примечание. Как указано в [RFC8126], назначения из пространства Private Use обычно бесполезны для широкого взаимодействия (совместимости). Использующие значения из этого диапазона принимают на себя ответственность за предотвращение конфликтов значения (в предполагаемой области применения). Для более широких экспериментов доступны временно выделяемые значения.

11. Новый тип сообщений Session Ticket TLS Handshake

Для согласования с реализациями TLS и номенклатурой именования других типов сообщений Handshake агентство IANA:

- переименовало запись 4 в реестре TLS HandshakeType на new_session_ticket (было NewSessionTicket) [RFC5077];
- добавило ссылку на этот документе в столбец Reference для записи 4 в реестре TLS HandshakeType.

12. Реестр TLS Exporter Labels

В помощь рецензентам, начинающим с реестра, агентство IANA внесло 2 добавления.

- Примечание в реестр TLS Exporter Labels.

  Примечание. В [RFC5705] определены экспортёры ключевого материала для TLS в терминах TLS PRF. В [RFC8446] функция PRF была заменена на HKDF, что потребовало новой конструкции. Интерфейс экспортёра не изменился, однако значения рассчитываются иначе.
- Столбец Recommended в реестре TLS Exporter Labels. Создана приведённая ниже таблица со статусом Y для Standards Track RFC и N для остальных. Значение N в столбце Recommended устанавливается, если явно не запрошено иное, а установка Y выполняется по процедуре Standards Action [RFC8126]. Для смены Y на N **требуется** процедура IESG Approval.

Значение экспортёра	***Рекомендуется***
client finished	Y
server finished	Y
master secret	Y
key expansion	Y
client EAP encryption	Y
ttls keying material	N
ttls challenge	N

EXTRACTOR-dtls_srtp	Y
EXPORTER_DTLS_OVER_SCTP	Y
EXPORTER: teap session key seed	Y

В качестве дополнительных сведений для назначенных экспертов агентство IANA добавило два примечания.

Примечание. Роль назначенного эксперта описана в RFC 8447. Назначенный эксперт [RFC8126] обеспечивает публичную доступность спецификации. Для этого достаточно иметь документ Internet-Draft (который отправлен, но не опубликован в RFC) или документ оного органа стандартизации, отраслевого консорциума, университета и т. п. Эксперт может представить более глубокую рецензию, но одобрение эксперта не следует рассматривать как поддержку данной экспортируемой метки. Эксперт также проверяет, что метка является строкой печатных символов ASCII, начинающейся с EXPORTER. Агентство IANA **должно** также проверять, что метка не является префиксом другой метки (например, метка key или master secretary недопустима).

Примечание. Если элемент не помечен как Recommended, это не обязательно говорит о его изъянах, а указывает лишь, что элемент не прошёл процедуру согласования IETF, имеет ограниченную применимость или предназначен для использования в особых (конкретных) случаях.

Агентство IANA обновило ссылки в этом реестре, добавив данный документ.

13. Добавление отсутствовавшего элемента в реестр TLS Alerts

Агентство IANA добавило приведённую ниже строку в реестр TLS Alerts (её пропустили в инструкциях для IANA [RFC7301]).

120 no_application_protocol Y [RFC7301] [RFC8447]

14. Типы сертификатов TLS

Опыт показывает, что процедура IETF Consensus для TLS Certificate Types Identifiers слишком строга. Рабочая группа приняла решение о замене процедуры на Specification Required [RFC8126] с сохранением некоторой части кодов для приватного использования. В результате реестр TLS Certificate Types Identifiers был обновлён IANA, как указано ниже.

- Изменена процедура регистрации.

  Значения от 0 до 223 (десятичное) выделяются по процедуре Specification Required [RFC8126], значения из диапазона 224-255 (десятичные) зарезервированы для приватного использования (Private Use) [RFC8126].

- В реестр добавлен столбец Recommended. Для X.509 и Raw Public Key в нем указано значение Y, для прочих - N. Значение N в столбце Recommended устанавливается, если явно не запрошено иное, а установка Y выполняется по процедуре Standards Action [RFC8126]. Для смены Y на N требуется процедура IESG Approval.

Назначение экспертов дополнительно описано в разделе 17.

Агентство IANA добавило приведённые ниже примечания.

Примечание. Роль назначенного эксперта описана в RFC 8447. Назначенный эксперт [RFC8126] обеспечивает публичную доступность спецификации. Для этого достаточно иметь документ Internet-Draft (который отправлен, но не опубликован в RFC) или документ оного органа стандартизации, отраслевого консорциума, университета и т. п. Эксперт может представить более глубокую рецензию, но одобрение эксперта не следует рассматривать как поддержку данного типа сертификата.

Примечание. Если элемент не помечен как Recommended, это не обязательно говорит о его изъянах, а указывает лишь, что элемент не прошёл процедуру согласования IETF, имеет ограниченную применимость или предназначен для использования в особых (конкретных) случаях.

Агентство IANA обновило ссылки в этом реестре, добавив данный документ.

15. «Осиротевшие» реестры

Чтобы пояснить исключение для (D)TLS 1.3 некоторых реестров (они сохраняются лишь для (D)TLS более ранних версий, агентство IANA внесло приведённые ниже изменения.

- В реестр TLS Compression Method Identifiers [RFC3749] добавлено приведённое ниже примечание.

Примечание. Значение 0 (NULL) является единственным значением из этого реестра, применимым к (D)TLS версии 1.3 и выше.

- В реестры TLS HashAlgorithm [RFC5246] и TLS SignatureAlgorithm [RFC5246] добавлено приведённое ниже примечание.

Примечание. Значения из этого реестра применимы лишь к протоколам (D)TLS до версии 1.3. Значения для (D)TLS 1.3 и более новых версий приведены в реестре TLS SignatureScheme.

- Обновлено поле Reference в реестрах TLS Compression Method Identifiers, TLS HashAlgorithm, TLS SignatureAlgorithm с указанием ссылки на этот документ.

- Обновлён реестр TLS HashAlgorithm для указания значений 7 и 9-223 как резервных (Reserved) и реестр TLS SignatureAlgorithm для указания значений 4-6 и 9-223 как Reserved.

- Добавлено приведённое ниже примечание в реестр TLS ClientCertificateType Identifiers [RFC5246].

Примечание. Значения из этого реестра применимы лишь к протоколам (D)TLS до версии 1.3.

Несмотря на то, что реестры TLS HashAlgorithm и SignatureAlgorithm «осиротели», важность предупреждения разработчиков предшествующих (до TLS 1.3) реализации об опасности слепого внедрения криптоалгоритмов не

исчезла. Поэтому агентство IANA добавило в реестры TLS HashAlgorithm и SignatureAlgorithm приведённое ниже примечание.

> Предупреждение. Криптографические алгоритмы и параметры могут с течением времени взломаны или сочтены слабыми. Слепая реализация указанных в списке поддерживаемых групп не рекомендуется. Разработчикам и пользователям необходимо проверять наличие и статус алгоритмов в списке для обеспечения требуемого уровня защиты.

16. Дополнительные замечания

Агентство IANA добавило приведённые ниже примечания в реестр TLS SignatureScheme.

> Предупреждение. Криптографические алгоритмы и параметры могут с течением времени взломаны или сочтены слабыми. Слепая реализация указанных в списке поддерживаемых групп не рекомендуется. Разработчикам и пользователям необходимо проверять наличие и статус алгоритмов в списке для обеспечения требуемого уровня защиты.
>
> Примечание. Как указано в [RFC8126], назначения из пространства Private Use обычно бесполезны для широкого взаимодействия (совместимости). Использующие значения из этого диапазона принимают на себя ответственность за предотвращение конфликтов значения (в предполагаемой области применения). Для более широких экспериментов доступны временно выделяемые значения.

Агентство IANA добавило приведённые ниже примечания в реестр TLS PskKeyExchangeMode.

> Примечание. Если элемент не помечен как Recommended, это не обязательно говорит о его изъянах, а указывает лишь, что элемент не прошёл процедуру согласования IETF, имеет ограниченную применимость или предназначен для использования в особых (конкретных) случаях.
>
> Примечание. Роль назначенного эксперта описана в RFC 8447. Назначенный эксперт [RFC8126] обеспечивает публичную доступность спецификации. Для этого достаточно иметь документ Internet-Draft (который отправлен, но не опубликован в RFC) или документ оного органа стандартизации, отраслевого консорциума, университета и т. п. Эксперт может представить более глубокую рецензию, но одобрение эксперта не следует рассматривать как поддержку данного режима обмена ключами.

17. Назначенные эксперты

Запросы на выделение значений по процедуре Specification Required [RFC8126] регистрируются после 3-недельного периода рассмотрения в почтовой конференции <tls-reg-review@ietf.org> по рекомендации одного или нескольких назначенных экспертов. Однако для выделения значений до публикации назначенные эксперты могут утвердить регистрацию, как только убедятся в том, что спецификация будет опубликована.

В регистрационных запросах, направляемых в почтовую конференцию, **следует** указывать подходящую тему (subject), например, Request to register value in TLS bar registry (запрос на регистрацию в реестре TLS bar).

В течение периода рецензирования назначенные эксперты одобрят или отклонят запрос на регистрацию, сообщая своё решение в конференции и передавая его в IANA. В отказ **следует** включать разъяснение причины и, по возможности, предложения для обеспечения успешной регистрации. Запросы на регистрацию, не обработанные в течение 21 дня, могут быть представлены в IESG (через почтовую конференцию <iesg@ietf.org>) для разрешения проблемы.

Критерии, которые **следует** применять назначенным экспертам, включают определение дублирования предложенной регистрацией имеющейся функциональности, её применимость и полезность, а также чёткость описания.

Агентство IANA **должно** воспринимать обновления реестров только от назначенных экспертов и все регистрационные запросы **следует** направлять в почтовую конференцию (mailing list) для рецензирования.

Предлагается назначать несколько экспертов, которые способны представить перспективы разных приложений с использованием спецификации, чтобы обеспечить широкого анализа решений о регистрации. В случаях, когда решение о регистрации может быть воспринято как следствие конфликта интересов для конкретного эксперта, этому эксперту **следует** полагаться на мнение других экспертов.

18. Вопросы безопасности

Переход к процедуре Specification Required вместо IETF Review снижает объем рецензирования, предоставляемого рабочей группой для шифров и поддерживаемых групп. Это изменение отражает реальность в том смысле, что рабочая группа по существу не проводила криптографического анализа шифров и поддерживаемых групп. Особенно это касалось национальных шифронаборов.

Рекомендуемые алгоритмы считаются защищёнными для общего применения на момент регистрации, однако с течением времени они могут быть взломаны или сочтены слабыми. Статус Recommended в реестре может отставать от последних достижений криптоанализа. Разработчики и пользователи должны убедиться, что перечисленные криптоалгоритмы продолжают обеспечивать ожидаемый уровень защиты.

Назначенные эксперты обеспечивают публичную доступность спецификации. Они могут предоставлять более глубокий анализ, но его не следует считать одобрением (продвижением) шифра, расширения, поддерживаемой группы и т. п.

19. Взаимодействие с IANA

Этот документ целиком посвящён связанным с TLS реестрам IANA.

20. Литература

20.1. 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>.

[RFC3749] Hollenbeck, S., "Transport Layer Security Protocol Compression Methods", RFC 3749, DOI 10.17487/RFC3749, May 2004, <https://www.rfc-editor.org/info/rfc3749>.

[RFC4680] Santesson, S., "TLS Handshake Message for Supplemental Data", RFC 4680, DOI 10.17487/RFC4680, October 2006, <https://www.rfc-editor.org/info/rfc4680>.

[RFC5077] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 5077, DOI 10.17487/RFC5077, January 2008, <https://www.rfc-editor.org/info/rfc5077>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC5705] Rescorla, E., "Keying Material Exporters for Transport Layer Security (TLS)", RFC 5705, DOI 10.17487/RFC5705, March 2010, <https://www.rfc-editor.org/info/rfc5705>.

[RFC5878] Brown, M. and R. Housley, "Transport Layer Security (TLS) Authorization Extensions", RFC 5878, DOI 10.17487/RFC5878, May 2010, <https://www.rfc-editor.org/info/rfc5878>.

[RFC6520] Seggelmann, R., Tuexen, M., and M. Williams, "Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension", RFC 6520, DOI 10.17487/RFC6520, February 2012, <https://www.rfc-editor.org/info/rfc6520>.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, DOI 10.17487/RFC7301, July 2014, <https://www.rfc-editor.org/info/rfc7301>.

[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>.

[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>.

20.2. Дополнительная литература

[RFC4366] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 4366, DOI 10.17487/RFC4366, April 2006, <https://www.rfc-editor.org/info/rfc4366>.

[RFC6961] Pettersen, Y., "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension", RFC 6961, DOI 10.17487/RFC6961, June 2013, <https://www.rfc-editor.org/info/rfc6961>.

[RFC8422] Nir, Y., Josefsson, S., and M. Pegourie-Gonnard, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier", RFC 8422, DOI 10.17487/RFC8422, August 2018, <https://www.rfc-editor.org/info/rfc8422>.

[TOKBIND] Popov, A., Nystrom, M., Balfanz, D., and A. Langley, "Transport Layer Security (TLS) Extension for Token Binding Protocol Negotiation", Work in Progress[1], draft-ietf-tokbind-negotiation-14, May 2018.

Адреса авторов

Joe Salowey
Tableau Software
Email: joe@salowey.net

Sean Turner
sn3rd
Email: sean@sn3rd.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1]Опубликовано в RFC 8472. *Прим. перев.*