Internet Engineering Task Force (IETF) N. Aviram
Request for Comments: 10015 July 2026
Updates: 4162, 4279, 4346, 4785, 5246, 5288,
5289, 5469, 5487, 5932, 6209, 6347,
6367, 6655, 7905, 8422, 9325
Category: Standards Track
ISSN: 2070-1721

Deprecating Obsolete Key Exchange Methods in TLS 1.2 and DTLS 1.2

Отмена устаревших методов обмена ключами в TLS 1.2 и DTLS 1.2

Аннотация

Для (D)TLS 1.2 этот документ отменяет (deprecate) использование двух методов обмена ключами - метод Диффи-Хеллмана (Diffie-Hellman или DH) над конечным полем и RSA. Документ также рекомендует не применять шифры DH на основе эллиптических кривых (Elliptic Curve Diffie-Hellman или ECDH).

Эти предписания относятся только к (D)TLS 1.2, поскольку (D)TLS 1.0 и TLS 1.1 были отменены RFC 8996, а (D)TLS 1.3 не использует соответствующие алгоритмы и параметры конфигурации. DTLS версии 1.1 не существует.

Документ обновляет RFC 4162, 4279, 4346, 4785, 5246, 5288, 5289, 5469, 5487, 5932, 6209, 6347, 6367, 6655, 7905, 8422, 9325, исключая или не рекомендуя применение шифров, использующих упомянутые выше мотоды обмена ключами в соединениях (D)TLS 1.2.

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/rfc10015.

Оглавление

1. Введение

(D)TLS 1.2 поддерживает большой набор алгоритмов обмена ключами, включая RSA, метод Диффи-Хеллмана (Diffie-Hellman или DH) над конечным полем, метод DH с эллиптическими кривыми (Elliptic Curve Diffie-Hellman или ECDH).

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

Обмен ключами DH для любой группы может быть как эфемерным, так и неэфемерным. В неэфемерных алгоритмах DH применяются статические открытые ключи DH из сертификатов проверяющего подлинность узла (см. [RFC4492]), а в эфемерных - краткосрочные открытые ключи, переданные в согласовании и аутентифицируемые по сертификату партнёра. Эфемерные и неэфемерные алгоритмы DH над конечным полем называют DHE и DH (или FFDHE и FFDH), соответственно, а эфемерные и неэфемерные алгоритмы DH над эллиптическими кривыми - ECDHE и ECDH, соответственно [RFC4492].

В общем случае неэфемерные шифронаборы не рекомендуются из-за недостаточной безопасности в будущем (forward secrecy). Кроме того, как показала атака Raccoon [RACCOON] на DH над конечным полем, неоднократное применение открытых ключей (неэфемерные шифронаборы или эфемерные шифры с повторным использованием ключей) может приводить к сбоям в каналах синхронизации, которые могут приводить к утечке секретов соединения. Для ECDH атаки с применением недействительной кривой похожим способом используют уязвимость повторного использования секретов для взлома защиты [ICA], что ещё раз демонстрирует риск неоднократного применения ключей. Хотя при внедрении можно избежать обоих типов побочных каналов, опыт показывает, что на практике реализации могут оказаться не в состоянии предотвратить такие атаки из-за сложности и числа требуемых мер смягчения.

Кроме того, обмену ключей RSA присущи проблемы безопасности, которые не зависят от выбора реализации, а также проблемы, возникающие исключительно из-за сложности корректной реализации мер защиты.

Проблемы, затрагивающие FFDHE в (D)TLS 1.2, в общих чертах указаны ниже.

1. FFDHE страдает от проблем функциональной совместимости из-за отсутствия механизма согласования группы, а некоторые реализации поддерживают лишь группы малого размера (см. раздел 1 в [RFC7919]).
2. В группах FFDHE могут быть малые подгруппы, что делает возможными несколько атак [SUBGROUPS]. При использовании нестандартной пользовательской (custom) группы FFDHE клиент в согласовании не может практически убедиться, что выбранная сервером группа не имеет этой проблемы. Для таких согласований также нет механизма возврата к другим параметрам обмена ключами, приемлемым для клиента. Пользовательские группы FFDHE широко распространены (на основе рекомендаций [WEAK-DH]), поэтому клиенты не могут просто отвергать согласования с нестандартными и потенциально опасными группами.
3. На практике некоторые операторы применяют 1024-битовые группы FFDHE, поскольку это максимальный размер, обеспечивающий широкую поддержку (см. раздел 1 в [RFC7919]). При таком размере остаётся лишь незначительный запас безопасности по сравнению с текущим рекордом дискретного логалифимирования в 795 битов [DLOG795].
4. Возвращаясь к предыдущему пункту, можно сказать, что незначительное число очень больших расчётов позволяют злоумышленнику задёшево расшифровать относительно большую часть трафика FFDHE (а именно, трафик, зашифрованный с использованием частично стандартизованных групп) [WEAK-DH].
5. Когда секреты не полностью эфемерны, алгоритм FFDHE подвержен атакам Raccoon по побочным каналам [RACCOON] (отметим, что алгоритм FFDH по своей природе уязвим к атакам Raccoon, пока не применяются методы смягчения с постояннным временем выполнения).

Проблемы, затрагивающие обмен ключами RSA в (D)TLS 1.2 указаны ниже.

1. Обмен ключами RSA по своему устройству не обеспечивает безопасности в будущем.
2. Обмен ключами RSA может быть уязвим для атак Bleichenbacher [BLEI]. Опыт показывает, что варианты этой атаки появляются каждые несколько лет, поскольку корректная реализация мер противодействия сложна (см. [ROBOT], [NEW-BLEI], [DROWN]).
3. Кроме того, в (D)TLS 1.2 нет механизма разделения ключей по доменам, поэтому одна точка, уязвимая для атак Bleichenbacher, будет влиять на все конечные точки, применяющие тот же ключ RSA (см. [XPROT] и [DROWN]).

Этот документ обновляет [RFC4162], [RFC4279], [RFC4346], [RFC4785], [RFC5246], [RFC5288], [RFC5289], [RFC5469], [RFC5487], [RFC5932], [RFC6209], [RFC6347], [RFC6367], [RFC6655], [RFC7905], [RFC8422], [RFC9325] для устранения указанных выше проблем путём отмены или исключения рекомендаций для затагиваемых шифронаборов, как указано в параграфах 5.1 - 5.5.

В BCP 195 [RFC8996] [RFC9325] приведены последние рекомендации IETF для пользователей протоколов (D)TLS (в частности, (D)TLS 1.2) и данный документ обновляет [RFC9325] в нескольких пунктах. Точные различия указаны в разделе 6. Остальные рекомендации в BCP остаются в силе.

1.1. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не следует** (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.

2. Неэфемерные методы Диффи-Хеллмана

Клиентам **недопустимо** предлагать, а серверам **недопустимо** выбирать неэфемерные шифры FFDH в соединениях (D)TLS 1.2 (отметим, что (D)TLS 1.0 и TLS 1.1 отменены [RFC8996], а (D)TLS 1.3 не поддерживает FFDH [RFC9846] [RFC9147]). Это относится ко всем шифронаборам, указанным в таблице 1 параграфа 5.1.

Клиентам **не следует** предлагать, а серверам **не следует** выбирать неэфемерные шифры ECDH в соединениях (D)TLS 1.2 (это требование уже указано в [RFC9325]; отметим, что (D)TLS 1.0 и TLS 1.1 отменены [RFC8996], а (D)TLS 1.3 не поддерживает ECDH [RFC9846] [RFC9147]). Это относится ко всем шифрам, указанным в таблице 2 параграфа 5.2.

Кроме того, во избежание применения неэфемерных методов DH, клиентам **не следует** использовать, а серверам **не следует** воспринимать сертификаты с фиксированными параметрами DH. К этим типам сертификатов относятся rsa_fixed_dh, dss_fixed_dh, rsa_fixed_ecdh, ecdsa_fixed_ecdh, как указано в параграфе 5.5. Эти значения применимы лишь в (D)TLS версии 1.2 и ниже.

3. Эфемерные методы Диффи-Хеллмана над конечным полем

Клиентам **недопустимо** предлагать, а серверам **недопустимо** выбирать шифры FFDHE в соединениях (D)TLS 1.2. Это относится ко всем шифрам, указанным в таблице 3 параграфа 5.3. (отметим, что (D)TLS 1.0 и TLS 1.1 отменены [RFC8996]). Шифры FFDHE в (D)TLS 1.3 не подвержены проблемам, отмеченным в разделе 1 (см. [RFC9846] и [RFC9147], поэтому клиенты и серверы **могут** предлагать шифры FFDHE в соединениях (D)TLS 1.3.

4. RSA

Клиентам **недопустимо** предлагать, а серверам **недопустимо** выбирать шифры RSA в соединениях (D)TLS 1.2 (отметим, что (D)TLS 1.0 и TLS 1.1 отменены [RFC8996], а (D)TLS 1.3 не поддерживает статический RSA [RFC9846] [RFC9147]). Это относится ко всем шифрам, указанным в таблице 4 параграфа 5.4. Отметим, что эти шифры были ранее помечены как нерекомендуемые в реестре TLS Cipher Suites [TLS-REGISTRY].

5. Шифры и идентификаторы TLS ClientCertificateType

В следующих параграфах задано указание «D» в столбце Recommended (рекомендуется) реестров TLS Cipher Suites и TLS ClientCertificateType Identifiers [TLS-REGISTRY]. Использование «D» описано в [RFC9847].

5.1. Шифры DH, отменённые этим документом

Агентство IANA установило значение «D» в столбце Recommended и добавило ссылку на этот документ в указанные ниже записи реестра TLS Cipher Suites [TLS-REGISTRY].

Таблица 1.

Шифр	*Документы*
TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	[RFC4346]
TLS_DH_DSS_WITH_DES_CBC_SHA	[RFC8996]
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	[RFC5246]
TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	[RFC4346]
TLS_DH_RSA_WITH_DES_CBC_SHA	[RFC8996]
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	[RFC5246]
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	[RFC4346] [RFC6347]
TLS_DH_anon_WITH_RC4_128_MD5	[RFC5246] [RFC6347]
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	[RFC4346]
TLS_DH_anon_WITH_DES_CBC_SHA	[RFC8996]
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	[RFC5246]
TLS_DH_DSS_WITH_AES_128_CBC_SHA	[RFC5246]
TLS_DH_RSA_WITH_AES_128_CBC_SHA	[RFC5246]
TLS_DH_anon_WITH_AES_128_CBC_SHA	[RFC5246]
TLS_DH_DSS_WITH_AES_256_CBC_SHA	[RFC5246]
TLS_DH_RSA_WITH_AES_256_CBC_SHA	[RFC5246]
TLS_DH_anon_WITH_AES_256_CBC_SHA	[RFC5246]
TLS_DH_DSS_WITH_AES_128_CBC_SHA256	[RFC5246]
TLS_DH_RSA_WITH_AES_128_CBC_SHA256	[RFC5246]
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	[RFC5932]
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	[RFC5932]
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	[RFC5932]
TLS_DH_DSS_WITH_AES_256_CBC_SHA256	[RFC5246]
TLS_DH_RSA_WITH_AES_256_CBC_SHA256	[RFC5246]
TLS_DH_anon_WITH_AES_128_CBC_SHA256	[RFC5246]
TLS_DH_anon_WITH_AES_256_CBC_SHA256	[RFC5246]
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	[RFC5932]
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	[RFC5932]
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	[RFC5932]
TLS_DH_DSS_WITH_SEED_CBC_SHA	[RFC4162]
TLS_DH_RSA_WITH_SEED_CBC_SHA	[RFC4162]
TLS_DH_anon_WITH_SEED_CBC_SHA	[RFC4162]
TLS_DH_RSA_WITH_AES_128_GCM_SHA256	[RFC5288]
TLS_DH_RSA_WITH_AES_256_GCM_SHA384	[RFC5288]
TLS_DH_DSS_WITH_AES_128_GCM_SHA256	[RFC5288]
TLS_DH_DSS_WITH_AES_256_GCM_SHA384	[RFC5288]
TLS_DH_anon_WITH_AES_128_GCM_SHA256	[RFC5288]
TLS_DH_anon_WITH_AES_256_GCM_SHA384	[RFC5288]
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256	[RFC5932]
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256	[RFC5932]
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	[RFC5932]
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256	[RFC5932]
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256	[RFC5932]
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	[RFC5932]
TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256	[RFC6209]
TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384	[RFC6209]
TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256	[RFC6209]
TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384	[RFC6209]

TLS_DH_anon_WITH_ARIA_128_CBC_SHA256	[RFC6209]
TLS_DH_anon_WITH_ARIA_256_CBC_SHA384	[RFC6209]
TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256	[RFC6209]
TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384	[RFC6209]
TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256	[RFC6209]
TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384	[RFC6209]
TLS_DH_anon_WITH_ARIA_128_GCM_SHA256	[RFC6209]
TLS_DH_anon_WITH_ARIA_256_GCM_SHA384	[RFC6209]
TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256	[RFC6367]
TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384	[RFC6367]
TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256	[RFC6367]
TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384	[RFC6367]
TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256	[RFC6367]
TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384	[RFC6367]

5.2. Шифры ECDH, использовать которые этот документ не рекомендует

В [RFC9325] указано, что реализациям **не следует** согласовывать указанные в таблице 2 шифры, поэтому они помечены как «N» в колонке Recommended реестра IANA TLS Cipher Suites [TLS-REGISTRY]. В соответствии с этим документом агентство IANA установило значение «D» в столбце Recommended для согласования с [RFC9847] и указало ссылку на этот документ. Данный документ обосновывает отказ от этих шифров, а также содержит ссылки на анализ и атаки, где показаны соответствующие риски (см. раздел 8).

Таблица 2.

Шифр	***Документы***
TLS_ECDH_ECDSA_WITH_NULL_SHA	[RFC8422]
TLS_ECDH_ECDSA_WITH_RC4_128_SHA	[RFC8422] [RFC6347]
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	[RFC8422]
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	[RFC8422]
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	[RFC8422]
TLS_ECDH_RSA_WITH_NULL_SHA	[RFC8422]
TLS_ECDH_RSA_WITH_RC4_128_SHA	[RFC8422] [RFC6347]
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	[RFC8422]
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	[RFC8422]
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	[RFC8422]
TLS_ECDH_anon_WITH_NULL_SHA	[RFC8422]
TLS_ECDH_anon_WITH_RC4_128_SHA	[RFC8422] [RFC6347]
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	[RFC8422]
TLS_ECDH_anon_WITH_AES_128_CBC_SHA	[RFC8422]
TLS_ECDH_anon_WITH_AES_256_CBC_SHA	[RFC8422]
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	[RFC5289]
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	[RFC5289]
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	[RFC5289]
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	[RFC5289]
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	[RFC5289]
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	[RFC5289]
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	[RFC5289]
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	[RFC5289]
TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256	[RFC6209]
TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384	[RFC6209]
TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256	[RFC6209]
TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384	[RFC6209]
TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256	[RFC6209]
TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384	[RFC6209]
TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256	[RFC6209]
TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384	[RFC6209]
TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	[RFC6367]
TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	[RFC6367]
TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256	[RFC6367]
TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384	[RFC6367]
TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	[RFC6367]
TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	[RFC6367]
TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256	[RFC6367]
TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384	[RFC6367]

5.3. Шифры DHE, отменённые этим документом

Агентство IANA установило значение «D» в столбце Recommended и добавило ссылку на этот документ в указанные ниже записи реестра TLS Cipher Suites [TLS-REGISTRY]:

Таблица 3.

Шифр	***Документы***
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	[RFC4346]
TLS_DHE_DSS_WITH_DES_CBC_SHA	[RFC8996]
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	[RFC5246]
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	[RFC4346]
TLS_DHE_RSA_WITH_DES_CBC_SHA	[RFC8996]
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	[RFC5246]
TLS_DHE_PSK_WITH_NULL_SHA	[RFC4785]
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	[RFC5246]

TLS_DHE_RSA_WITH_AES_128_CBC_SHA	[RFC5246]
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	[RFC5246]
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	[RFC5246]
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	[RFC5246]
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	[RFC5932]
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	[RFC5932]
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	[RFC5246]
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	[RFC5246]
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	[RFC5246]
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	[RFC5932]
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	[RFC5932]
TLS_DHE_PSK_WITH_RC4_128_SHA	[RFC4279] [RFC6347]
TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA	[RFC4279]
TLS_DHE_PSK_WITH_AES_128_CBC_SHA	[RFC4279]
TLS_DHE_PSK_WITH_AES_256_CBC_SHA	[RFC4279]
TLS_DHE_DSS_WITH_SEED_CBC_SHA	[RFC4162]
TLS_DHE_RSA_WITH_SEED_CBC_SHA	[RFC4162]
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	[RFC5288]
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	[RFC5288]
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	[RFC5288]
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	[RFC5288]
TLS_DHE_PSK_WITH_AES_128_GCM_SHA256	[RFC5487]
TLS_DHE_PSK_WITH_AES_256_GCM_SHA384	[RFC5487]
TLS_DHE_PSK_WITH_AES_128_CBC_SHA256	[RFC5487]
TLS_DHE_PSK_WITH_AES_256_CBC_SHA384	[RFC5487]
TLS_DHE_PSK_WITH_NULL_SHA256	[RFC5487]
TLS_DHE_PSK_WITH_NULL_SHA384	[RFC5487]
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	[RFC5932]
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	[RFC5932]
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	[RFC5932]
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	[RFC5932]
TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256	[RFC6209]
TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384	[RFC6209]
TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256	[RFC6209]
TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384	[RFC6209]
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256	[RFC6209]
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384	[RFC6209]
TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256	[RFC6209]
TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384	[RFC6209]
TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256	[RFC6209]
TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384	[RFC6209]
TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256	[RFC6209]
TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384	[RFC6209]
TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	[RFC6367]
TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	[RFC6367]
TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256	[RFC6367]
TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384	[RFC6367]
TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256	[RFC6367]
TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384	[RFC6367]
TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256	[RFC6367]
TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384	[RFC6367]
TLS_DHE_RSA_WITH_AES_128_CCM	[RFC6655]
TLS_DHE_RSA_WITH_AES_256_CCM	[RFC6655]
TLS_DHE_RSA_WITH_AES_128_CCM_8	[RFC6655]
TLS_DHE_RSA_WITH_AES_256_CCM_8	[RFC6655]
TLS_DHE_PSK_WITH_AES_128_CCM	[RFC6655]
TLS_DHE_PSK_WITH_AES_256_CCM	[RFC6655]
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	[RFC7905]
TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256	[RFC7905]
TLS_PSK_DHE_WITH_AES_128_CCM_8	[RFC6655]
TLS_PSK_DHE_WITH_AES_256_CCM_8	[RFC6655]

5.4. Шифры RSA, отменённые этим документом

Агентство IANA установило значение «D» в столбце Recommended и добавило ссылку на этот документ в указанные ниже записи реестра TLS Cipher Suites [TLS-REGISTRY]:

Таблица 4.

Шифр	***Документы***
TLS_RSA_WITH_NULL_MD5	[RFC5246]
TLS_RSA_WITH_NULL_SHA	[RFC5246]
TLS_RSA_EXPORT_WITH_RC4_40_MD5	[RFC4346] [RFC6347]
TLS_RSA_WITH_RC4_128_MD5	[RFC5246] [RFC6347]
TLS_RSA_WITH_RC4_128_SHA	[RFC5246] [RFC6347]
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	[RFC4346]
TLS_RSA_WITH_IDEA_CBC_SHA	[RFC8996]
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	[RFC4346]
TLS_RSA_WITH_DES_CBC_SHA	[RFC8996]
TLS_RSA_WITH_3DES_EDE_CBC_SHA	[RFC5246]

TLS_RSA_PSK_WITH_NULL_SHA	[RFC4785]
TLS_RSA_WITH_AES_128_CBC_SHA	[RFC5246]
TLS_RSA_WITH_AES_256_CBC_SHA	[RFC5246]
TLS_RSA_WITH_NULL_SHA256	[RFC5246]
TLS_RSA_WITH_AES_128_CBC_SHA256	[RFC5246]
TLS_RSA_WITH_AES_256_CBC_SHA256	[RFC5246]
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	[RFC5932]
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	[RFC5932]
TLS_RSA_PSK_WITH_RC4_128_SHA	[RFC4279] [RFC6347]
TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA	[RFC4279]
TLS_RSA_PSK_WITH_AES_128_CBC_SHA	[RFC4279]
TLS_RSA_PSK_WITH_AES_256_CBC_SHA	[RFC4279]
TLS_RSA_WITH_SEED_CBC_SHA	[RFC4162]
TLS_RSA_WITH_AES_128_GCM_SHA256	[RFC5288]
TLS_RSA_WITH_AES_256_GCM_SHA384	[RFC5288]
TLS_RSA_PSK_WITH_AES_128_GCM_SHA256	[RFC5487]
TLS_RSA_PSK_WITH_AES_256_GCM_SHA384	[RFC5487]
TLS_RSA_PSK_WITH_AES_128_CBC_SHA256	[RFC5487]
TLS_RSA_PSK_WITH_AES_256_CBC_SHA384	[RFC5487]
TLS_RSA_PSK_WITH_NULL_SHA256	[RFC5487]
TLS_RSA_PSK_WITH_NULL_SHA384	[RFC5487]
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	[RFC5932]
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	[RFC5932]
TLS_RSA_WITH_ARIA_128_CBC_SHA256	[RFC6209]
TLS_RSA_WITH_ARIA_256_CBC_SHA384	[RFC6209]
TLS_RSA_WITH_ARIA_128_GCM_SHA256	[RFC6209]
TLS_RSA_WITH_ARIA_256_GCM_SHA384	[RFC6209]
TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256	[RFC6209]
TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384	[RFC6209]
TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256	[RFC6209]
TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384	[RFC6209]
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256	[RFC6367]
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384	[RFC6367]
TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256	[RFC6367]
TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384	[RFC6367]
TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256	[RFC6367]
TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384	[RFC6367]
TLS_RSA_WITH_AES_128_CCM	[RFC6655]
TLS_RSA_WITH_AES_256_CCM	[RFC6655]
TLS_RSA_WITH_AES_128_CCM_8	[RFC6655]
TLS_RSA_WITH_AES_256_CCM_8	[RFC6655]
TLS_RSA_PSK_WITH_CHACHA20_POLY1305_SHA256	[RFC7905]

5.5. Идентификаторы TLS ClientCertificateType, отменённые этим документом

Агентство IANA установило значение «D» в столбце Recommended и добавило ссылку на этот документ в указанные ниже записи реестра TLS ClientCertificateType Identifiers [TLS-REGISTRY]:

Таблица 5.

Тип сертификата	***Документы***
rsa_fixed_dh (3)	[RFC5246] [RFC9847]
dss_fixed_dh (4)	[RFC5246] [RFC9847]
rsa_fixed_ecdh (65)	[RFC8422] [RFC9847]
ecdsa_fixed_ecdh (66)	[RFC8422] [RFC9847]

6. Обновления RFC 9325

Этот документ обновляет [RFC9325] в части использования (D)TLS 1.2, различия указаны в таблице 6 и относятся к параграфу 4.1 в [RFC9325].

Таблица 6.

	RFC 9325	***RFC 10015***
Неэфемерные FFDH	**Не следует**	**Недопустимо**
Неэфемерные ECDH	**Не следует**	Без изменений
Фиксированные типы сертификатов DH	Не указано	**Не следует**
Эфемерные FFDH	**Не следует**	**Недопустимо**
Статический RSA	**Не следует**	**Недопустимо**

7. Взаимодействие с IANA

Реестры TLS Cipher Suites и TLS ClientCertificateType Identifiers входят в группу Transport Layer Security (TLS) Parameters [TLS-REGISTRY]. Агентство IANA обновило записи реестра TLS Cipher Suites [TLS-REGISTRY] в соответствии с параграфами 5.1, 5.2, 5.3, 5.4, а также записи TLS ClientCertificateType Identifiers в соответствии с параграфом 5.5.

Для каждой записи, указанной в параграфах 5.1, 5.2, 5.3, 5.4, 5.5, агентство IANA указало в столбце Recommended значение «D» и включило ссылку на этот документ в столбец Reference. Использование значения «D» в столбце Recommended описано в [RFC9847].

8. Вопросы безопасности

Неэфемерные шифры DH над конечным полем (TLS_DH_*), а также неоднократное применение эфемерных ключей в шифрах DH над конечным полем запрещены из-за атак Raccoon [RACCOON]. Те и другие уже сочтены плохой

практикой, поскольку они не обеспечивают секретности в будущем (forward secrecy). Однако атаки Raccoon показали, что атаки по побочным временным каналам при обработке секретов TLS (premaster secret) могут приводить к раскрытию зашифрованного premaster secret.

Для неэфемерных шифров ECDH (TLS_ECDH_*) отсутствие секретности в будущим не только позволит расшифровать прошлые данные в случае взлома ключа, но и может способствовать широкому спектру атак, связанных с неоднократным использованием ключа, где злоумышленник многократно запрашивает криптографический секрет.

К этой категории относятся приведённые ниже примеры, но могут существовать и иные варианты атак.

1. Атаки с использованием недействительной кривой, где злоумышленник пользуется неоднократным применением ключей для повторяющихся запросов с целью получения ключа. Показано, что такие атаки возможны на практике применительно к реальным реализациям TLS [ICA].
2. Атаки по побочным каналам, где злоумышленник выясняет криптографический секрет на основе неоднократного применения ключа и дополнительного стороннего канала. Пример такой атаки дан в [MAY4].
3. Атаки с использованием отказа, основанные на неоднократном применении ключа и некорректных расчётах, для выяснения криптографического секрета. Пример такой атаки можно найти в [PARIS256].

Такие атаки часто зависят от реализации, как в приведённых выше примерах. Однако примеры показывают, что на практике сложно создать систему с неоднократным применением ключей и избежать таких атак. Отказ же от неоднократного применения ключей не только предотвращает расшифровку в случае компрометации ключа, но и позволяет избежать таких атак. Поэтому данный документ не рекомендует повторно применять открытые ключи ECDH.

Для эфемерных DH над конечным полем в (D)TLS 1.2 (TLS_DHE_* и TLS_PSK_DHE_*), как отмечено выше, у клиентов нет практического способа поддержки этих шифров одновременно с гарантией согласования лишь приемлемых для клиента параметров безопасности. В (D)TLS 1.2 сервер выбирает группу DH и при этом превалируют пользовательские (custom) группы. Поэтому, как только клиент включит такие шифры в своё согласование, а сервер представит пользовательскую группу, клиент не сможет завершить согласование с приемлемой безопасностью. Проверка структуры группы для клиента является непомерно дорогой. Использование списка хорошо известных групп также непрактично, поскольку операторам серверов было рекомендовано обобщать свои пользовательские группы. Кроме того, не существует механизма согласования, позволяющего вернуться к другим параметрам, которые устраивают как клиента, так и сервер.

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

[RFC4162] Lee, H.J., Yoon, J.H., and J.I. Lee, "Addition of SEED Cipher Suites to Transport Layer Security (TLS)", RFC 4162, DOI 10.17487/RFC4162, September 2005, <https://www.rfc-editor.org/info/rfc4162>.

[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>.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, DOI 10.17487/RFC4346, April 2006, <https://www.rfc-editor.org/info/rfc4346>.

[RFC4785] Blumenthal, U. and P. Goel, "Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)", RFC 4785, DOI 10.17487/RFC4785, January 2007, <https://www.rfc-editor.org/info/rfc4785>.

[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>.

[RFC5288] Salowey, J., Choudhury, A., and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS", RFC 5288, DOI 10.17487/RFC5288, August 2008, <https://www.rfc-editor.org/info/rfc5288>.

[RFC5289] Rescorla, E., "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)", RFC 5289, DOI 10.17487/RFC5289, August 2008, <https://www.rfc-editor.org/info/rfc5289>.

[RFC5469] Eronen, P., Ed., "DES and IDEA Cipher Suites for Transport Layer Security (TLS)", RFC 5469, DOI 10.17487/RFC5469, February 2009, <https://www.rfc-editor.org/info/rfc5469>.

[RFC5487] Badra, M., "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode", RFC 5487, DOI 10.17487/RFC5487, March 2009, <https://www.rfc-editor.org/info/rfc5487>.

[RFC5932] Kato, A., Kanda, M., and S. Kanno, "Camellia Cipher Suites for TLS", RFC 5932, DOI 10.17487/RFC5932, June 2010, <https://www.rfc-editor.org/info/rfc5932>.

[RFC6209] Kim, W., Lee, J., Park, J., and D. Kwon, "Addition of the ARIA Cipher Suites to Transport Layer Security (TLS)", RFC 6209, DOI 10.17487/RFC6209, April 2011, <https://www.rfc-editor.org/info/rfc6209>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[RFC6367] Kanno, S. and M. Kanda, "Addition of the Camellia Cipher Suites to Transport Layer Security (TLS)", RFC 6367, DOI 10.17487/RFC6367, September 2011, <https://www.rfc-editor.org/info/rfc6367>.

[RFC6655] McGrew, D. and D. Bailey, "AES-CCM Cipher Suites for Transport Layer Security (TLS)", RFC 6655, DOI 10.17487/RFC6655, July 2012, <https://www.rfc-editor.org/info/rfc6655>.

[RFC7905] Langley, A., Chang, W., Mavrogiannopoulos, N., Strombergson, J., and S. Josefsson, "ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)", RFC 7905, DOI 10.17487/RFC7905, June 2016, <https://www.rfc-editor.org/info/rfc7905>.

[RFC7919] Gillmor, D., "Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)", RFC 7919, DOI 10.17487/RFC7919, August 2016, <https://www.rfc-editor.org/info/rfc7919>.

[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>.

[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>.

[RFC8996] Moriarty, K. and S. Farrell, "Deprecating TLS 1.0 and TLS 1.1", BCP 195, RFC 8996, DOI 10.17487/RFC8996, March 2021, <https://www.rfc-editor.org/info/rfc8996>.

[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>.

[RFC9325] Sheffer, Y., Saint-Andre, P., and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 9325, DOI 10.17487/RFC9325, November 2022, <https://www.rfc-editor.org/info/rfc9325>.

[RFC9846] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 9846, DOI 10.17487/RFC9846, July 2026, <https://www.rfc-editor.org/info/rfc9846>.

[RFC9847] Salowey, J. and S. Turner, "IANA Registry Updates for TLS and DTLS", RFC 9847, DOI 10.17487/RFC9847, December 2025, <https://www.rfc-editor.org/info/rfc9847>.

9.2. Дополнительная литература

[BLEI] Bleichenbacher, D., "Chosen Ciphertext Attacks against Protocols Based on the RSA Encryption Standard PKCS #1", Advances in Cryptology -- CRYPTO'98, Lecture Notes in Computer Science, vol. 1462, pp. 1-12, DOI 10.1007/BFb0055716, 1998, <https://doi.org/10.1007/BFb0055716>.

[DLOG795] Boudot, F., Gaudry, P., Guillevic, A., Heninger, N., Thomé, E., and P. Zimmermann, "Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment", Cryptology ePrint Archive, Paper 2020/697, DOI 10.1007/978-3-030-56880-1_3, 17 August 2020, <https://eprint.iacr.org/2020/697>.

[DROWN] Aviram, N., Schinzel, S., Somorovsky, J., Heninger, N., Dankel, M., Steube, J., Valenta, L., Adrian, D., Halderman, J. A., Dukhovni, V., Käsper, E., Cohney, S., Engels, S., Paar, C., and Y. Shavitt, "DROWN: Breaking TLS using SSLv2", Proceedings of the 25th USENIX Security Symposium, August 2016, <https://drownattack.com/drown-attack-paper.pdf>.

[ICA] Jager, T., Schwenk, J., and J. Somorovsky, "Practical invalid curve attacks on TLS-ECDH", ESORICS 2015, Part I, Lecture Notes in Computer Science, vol. 9326, pp. 407-425, DOI 10.1007/978-3-319-24174-6_21, 21 September 2015, <https://link.springer.com/content/pdf/10.1007/978-3-319-24174-6_21.pdf>.

[MAY4] Genkin, D., Valenta, L., and Y. Yarom, "May the Fourth Be With You: A Microarchitectural Side Channel Attack on Several Real-World Applications of Curve25519", Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, DOI 10.1145/3133956.3134029, 30 October 2017, <https://dl.acm.org/doi/pdf/10.1145/3133956.3134029>.

[NEW-BLEI] Meyer, C., Somorovsky, J., Weiss, E., Schwenk, J., Schinzel, S., and E. Tews, "Revisiting SSL/TLS Implementations: New Bleichenbacher Side Channels and Attacks", Proceedings of the 23rd USENIX Security Symposium, August 2014, <https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-meyer.pdf>.

[PARIS256] Devlin, S. and F. Valsorda, "The PARIS256 Attack", 8 August 2018, <https://i.blackhat.com/us-18/Wed-August-8/us-18-Valsorda-Squeezing-A-Key-Through-A-Carry-Bit-wp.pdf>.

[RACCOON] Merget, R., Brinkmann, M., Aviram, N., Somorovsky, J., Mittmann, J., and J. Schwenk, "Raccoon Attack: Finding and Exploiting Most-Significant-Bit-Oracles in TLS-DH(E)", 9 September 2020, <https://raccoon-attack.com/RacoonAttack.pdf>.

[RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, DOI 10.17487/RFC4492, May 2006, <https://www.rfc-editor.org/info/rfc4492>.

[ROBOT] Boeck, H., Somorovsky, J., and C. Young, "Return Of Bleichenbacher's Oracle Threat (ROBOT)", Proceedings of the 27th USENIX Security Symposium, August 2018, <https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-bock.pdf>.

[SUBGROUPS] Valenta, L., Adrian, D., Sanso, A., Cohney, S., Fried, J., Hastings, M., Halderman, J. A., and N. Heninger, "Measuring small subgroup attacks against Diffie-Hellman", Cryptology ePrint Archive, Paper 2016/995, 17 October 2016, <https://eprint.iacr.org/2016/995/20161017:193515>.

[TLS-REGISTRY] IANA, "Transport Layer Security (TLS) Parameters", <https://www.iana.org/assignments/tls-parameters>.

[WEAK-DH] Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., Heninger, N., Springall, D., Thomé, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Béguelin, S., and P. Zimmermann, "Weak Diffie-Hellman and the Logjam Attack", October 2015, <https://weakdh.org/>.

[XPROT] Jager, T., Schwenk, J., and J. Somorovsky, "On the Security of TLS 1.3 and QUIC Against Weaknesses in PKCS#1 v1.5 Encryption", Proceedings of the 22nd ACM SIGSAC Conference on Computer and

Communications Security, pp. 1185-1196, DOI 10.1145/2810103.2813657, October 2015, <https://doi.org/10.1145/2810103.2813657>.

Благодарности

Этот документ в значительной мере основан на вкладе Кэрри Бартл (Carrie Bartle), которая написала большую часть текста и несколько раз представила его в рабочей группе IETF TLS.

Документ базируется также на обсуждениях в почтовой конференции TLS WG и предложениях Филиппо Вальсорды (Filippo Valsorda) после публикации об атаке Raccoon [RACCOON]. Спасибо Кристоффферу А. Вуду (Christopher A. Wood) за исходный черновик документа, а также Томасу Фоссати (Thomas Fossati), Шону Тёрнеру (Sean Turner), Джо Салоуи (Joe Salowey), Ярону Шеффферу (Yaron Sheffer), Кристиану Бухграберу (Christian Buchgraber), Джону Прюссу Мэттсону (John Preuß Mattsson) и Мануэлю Пегурье-Гуннара (Manuel Pégourié-Gonnard) за их отклики и предложения.

Адрес автора

Nimrod Aviram
Email: nimrod.aviram@gmail.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru