

Internet Engineering Task Force (IETF)
Request for Comments: 9847
Updates: 8447
Category: Standards Track
ISSN: 2070-1721

J. Salowey
CyberArk
S. Turner
sn3rd
December 2025

IANA Registry Updates for TLS and DTLS

Обновление реестров IANA для TLS и DTLS

Аннотация

Этот документ обновляет изменения в реестрах TLS и DTLS IANA, внесённые RFC 8447. Добавлено новое значение D (discouraged - не рекомендуется) в столбец Recommended некоторых реестров TLS и столбец Comment (комментарий) во все активные реестры, где его не было. Также обновлены инструкции для запросов на регистрацию.

Документ обновляет RFC 8447.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF¹ и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG². Дополнительные сведения о документах Internet Standard приведены в разделе 2 RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке <https://www.rfc-editor.org/info/rfc9847>.

Авторские права

Авторские права (Copyright (c) 2025) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (<http://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с пересмотренной лицензией BSD (Revised BSD License), как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Revised BSD License).

Оглавление

1. Введение.....	1
2. Уровни требований.....	2
3. Обновление значений столбца Recommended.....	2
3.1. Примечание для столбца Recommended.....	2
4. Реестр типов расширений TLS.....	2
5. Реестр шифров TLS.....	2
6. Реестр поддерживаемых групп TLS.....	3
7. Реестр меток экспортёров TLS.....	4
8. Реестр типов сертификатов TLS.....	4
9. Реестр алгоритмов хэширования TLS.....	4
10. Реестр алгоритмов подписи TLS.....	4
11. Реестр идентификаторов типа сертификата клиента TLS.....	5
12. Реестр режимов обмена ключами TLS PskKeyExchangeMode.....	5
13. Реестр схем подписи TLS.....	5
14. Добавление столбца Comment.....	5
15. Рецензия экспертов на документы IETF и IRTF.....	6
16. Регистрационные запросы.....	6
17. Вопросы безопасности.....	6
18. Взаимодействие с IANA.....	6
19. Нормативные документы.....	6
Адреса авторов.....	7

1. Введение

Этот документ предписывает IANA внести множество изменений в реестры, относящиеся к защите транспортного уровня (Transport Layer Security или TLS) и защите транспортного уровня дейтаграмм (Datagram Transport Layer Security или DTLS). Изменения обновляют данные, внесённые [RFC8447].

Спецификация добавляет новое значение D (discouraged - не рекомендуется) для столбца Recommended в некоторых реестрах TLS и столбца Comment в реестры, где его ещё нет.

Спецификация также обновляет инструкции для запросов регистрации.

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

2. Уровни требований

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

3. Обновление значений столбца *Recommended*

Этот документ обновляет столбец *Recommended* (рекомендовано), добавленный [RFC8447], значением D, указывающим что строка (значение) не рекомендуется. Возможные значения описаны ниже.

Y

Указывает наличие согласованного мнения IETF о том, что данный элемент **рекомендуется**. Это говорит лишь о том, что соответствующий механизм подходит для целей, для которых он был определён. Для понимания фактической пригодности механизма следует внимательно прочесть его документацию. IETF может рекомендовать механизмы с ограниченной применимостью, но будет предоставлять заявления о применимости с описанием всех имеющихся ограничений механизма или требуемых при его применении ограничений.

N

Указывает, что данный элемент не был оценён IETF и IETF не делает каких-либо заявлений о пригодности соответствующего механизма. Это не обязательно означает несовершенство механизма и говорит лишь об отсутствии консенсуса. IETF может принять решение о сохранении статуса N на основании ограниченной применимости элемента или ограничений на его использование.

D

Указывает, что данный элемент не рекомендуется применять. Это может использоваться для указания механизмов, при использовании которых могут возникать проблемы (например, слабая криптография или проблемы функциональной совместимости при внедрении). При указании статуса D с колонке Reference или Comment **должны** быть достаточные сведения о причинах такой маркировки. Разработчикам и пользователям **следует** ознакомиться с этими сведениями для понимания условий, при которых элемент **не следует** или **недопустимо** использовать.

Установка и изменение значения Y или D в столбце *Recommended* выполняется по процедуре IETF Standards Action с рецензией экспертов (Expert Review) или IESG Approval [RFC8126]. Не все элементы, заданные в Standards Track RFC требуют установки статуса Y или D. Для всех элементов с неуказанным статусом предполагается N. Столбец не заполняется для резервных и невыделенных значений, пока не появится соответствующая спецификация.

3.1. Примечание для столбца *Recommended*

В имеющихся реестрах есть примечания о значении столбца *Recommended*. Для описанных ниже реестров эти примечания обновлены описанием значения D, как показано ниже.

Примечание. Если в столбце *Recommended* указано значение N, это необязательно говорит о недостатках. Скорее это указывает, что элемент не прошёл процедуру согласования IETF, имеет ограниченную применимость или предназначен лишь для конкретных случаев. Если в столбце *Recommended* указано D, данный элемент не рекомендуется и его **не следует** или **недопустимо** применять (в зависимости от ситуации). Для лучшего понимания следует обратиться к приведённым ссылкам.

4. Реестр типов расширений TLS

С учётом изменений в столбце *Recommended* агентство IANA обновило реестр TLS ExtensionType Values:

- Скорректирована процедура регистрации в части значения столбца *Recommended*:
Установка и изменение значения Y или D в столбце *Recommended* выполняется по процедуре IETF Standards Action с рецензией экспертов или по процедуре IESG Approval [RFC8126].
- Добавлена ссылка на данный документ.
- Обновлён столбец *Recommended*, как показано ниже. В записи со значениями Y и N лишь добавлена ссылка на этот документ.

Таблица 1.

Значение	Имя расширения	Рекомендовано
4	truncated_hmac	D
40	Reserved	D
46	Reserved	D
53	connection_id(deprecated)	D

- Обновлено примечание к столбцу *Recommended* в соответствии с параграфом 3.1.
- Для truncated_hmac добавлена ссылка <https://www.iacr.org/archive/asiacrypt2011/70730368/70730368.pdf> в столбец Reference.
- Для показанных в таблице строк Reserved добавлена ссылка https://mailarchive.ietf.org/arch/msg/tls-reg-review/5BD62HBFjo_AsW-Y8ohVuWEe1qI/ в столбец Reference.

5. Реестр шифров TLS

Несколько категорий шифров не рекомендуются для общего пользования и помечены значением D. Шифронаборы, использующие NULL-шифрование, не обеспечивают конфиденциальности, обычно ожидаемой от TLS. Протоколы и приложения часто разрабатываются с учётом обеспечения конфиденциальности как свойства защиты и таких случаях недопустимо применять шифронаборы с NULL-шифрованием.

Наборы с пометкой EXPORT используют слабые шифры и не рекомендуются для TLS 1.1 [RFC4346].

Наборы с пометкой апон не обеспечивают аутентификации и уязвимы к атакам в пути, поэтому не рекомендуются для TLS 1.1 [RFC4346].

Шифр RC4 признан слабым и не рекомендуется [RFC7465]. DES и IDEA¹ не считаются безопасными для общего пользования и не рекомендуются [RFC5469]. Алгоритмы MD5 и SHA-1 также признаны небезопасными для общего пользования и не рекомендуются [RFC9155].

В соответствии с изменениями столбца Recommended агентство IANA обновило реестр TLS Cipher Suites.

- Скорректирована процедура регистрации в части значения столбца Recommended:
Установка и изменение значения Y или D в столбце Recommended выполняется по процедуре IETF Standards Action с рецензией экспертов или по процедуре IESG Approval [RFC8126].
- Добавлена ссылка на данный документ.
- Обновлен столбец Recommended, как показано ниже. В записи со значениями Y и N лишь добавлена ссылка на этот документ. Данный документ не меняет значений в столбце DTLS-OK.

Таблица 2.

Значение	Описание	Рекомендовано
0x00,0x1E	TLS_KRB5_WITH_DES_CBC_SHA	D
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA	D
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA	D
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5	D
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5	D
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5	D
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA	D
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA	D
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA	D
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5	D
0x00,0x2A	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5	D
0x00,0x2B	TLS_KRB5_EXPORT_WITH_RC4_40_MD5	D
0x00,0x2C	TLS_PSK_WITH_NULL_SHA	D
0x00,0x8A	TLS_PSK_WITH_RC4_128_SHA	D
0x00,0xB0	TLS_PSK_WITH_NULL_SHA256	D
0x00,0xB1	TLS_PSK_WITH_NULL_SHA384	D
0xC0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA	D
0xC0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	D
0xC0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA	D
0xC0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA	D
0xC0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA	D
0xC0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA	D
0xC0,0x3A	TLS_ECDHE_PSK_WITH_NULL_SHA256	D
0xC0,0x3B	TLS_ECDHE_PSK_WITH_NULL_SHA384	D
0xC0,0xB4	TLS_SHA256_SHA256	D
0xC0,0xB5	TLS_SHA384_SHA384	D

- Обновлено примечание к столбцу Recommended в соответствии с параграфом 3.1.

6. Реестр поддерживаемых групп TLS

В соответствии с изменениями столбца Recommended агентство IANA обновило реестр TLS Supported Groups.

- Скорректирована процедура регистрации в части значения столбца Recommended:
Установка и изменение значения Y или D в столбце Recommended выполняется по процедуре IETF Standards Action с рецензией экспертов или по процедуре IESG Approval [RFC8126].
- Добавлена ссылка на данный документ.
- Обновлен столбец Recommended, как показано ниже. В записи со значениями Y и N лишь добавлена ссылка на этот документ.

Таблица 3.

Значение	Описание	Рекомендовано
1	sect163k1	D
2	sect163r1	D
3	sect163r2	D
4	sect193r1	D
5	sect193r2	D
6	sect233k1	D
7	sect233r1	D
8	sect239k1	D
15	secp160k1	D
16	secp160r1	D
17	secp160r2	D
18	secp192k1	D
19	secp192r1	D
20	secp224k1	D
21	secp224r1	D

¹International Data Encryption Algorithm - международный алгоритм шифрования данных.

- Обновлено примечание к столбцу Recommended в соответствии с параграфом 3.1.
- Удалено примечание Elliptic curve groups (группы эллиптических кривых) из таблицы процедур регистрации.
- Для приведённых выше записей добавлена ссылка <https://datatracker.ietf.org/meeting/118/materials/slides-118-tls-rfc8447bis-00> в столбец Comment.

7. Реестр меток экспортёров TLS

Этот документ обновляет процедуру регистрации в реестре TLS Exporter Labels и выделение столбца Recommended.

- Процедура регистрации Specification Required заменена процедурой Expert Review.
Установка и изменение значения Y или D в столбце Recommended выполняется по процедуре IETF Standards Action с рецензией экспертов или по процедуре IESG Approval [RFC8126].
- Добавлена ссылка на данный документ.
- В записях со значениями Y и N столбец Recommended не изменён.
- Обновлено примечание к столбцу Recommended в соответствии с параграфом 3.1.
- Обновлена роль рецензии экспертов, как указано ниже.

Примечание. Роль назначенных экспертов описана в разделе 17 [RFC8447]. Хотя данный реестр не требует спецификации, [RFC8126] настоятельно рекомендует претендентам на регистрацию указывать ссылку на публично доступную спецификацию, в качестве таковой подходят Internet-Draft (размещён, но не опубликован как RFC), документ другого органа стандартизации, отраслевого консорциума, университета и т. п. Эксперты могут представить более глубокие обзоры, но их одобрение не следует считать одобрением метки экспортёра. Эксперты также проверяют, что метка представляет собой строку печатаемых символов ASCII, начинающуюся с EXPORTER. Агентство IANA **должно** убедиться, что метка не является префиксом какой-либо другой метки. Например, запрещены метки key и master secretary.

- Столбец Note переименован в Comment.

8. Реестр типов сертификатов TLS

В соответствии с изменением для столбца Recommended агентство IANA обновило реестр TLS Certificate Types.

- Скорректирована процедура регистрации в части значения столбца Recommended.
Установка и изменение значения Y или D в столбце Recommended выполняется по процедуре IETF Standards Action с рецензией экспертов или по процедуре IESG Approval [RFC8126].
- Добавлена ссылка на данный документ.
- В записях со значениями Y и N столбец Recommended не изменён.
- Обновлено примечание к столбцу Recommended в соответствии с параграфом 3.1.

9. Реестр алгоритмов хэширования TLS

TLS 1.0 и TLS 1.1 признаны устаревшими [RFC8996], TLS 1.2 будет применяться ещё некоторое время. В соответствии с изменением для столбца Recommended агентство IANA обновило реестр TLS HashAlgorithm.

- Скорректирована процедура регистрации в части значения столбца Recommended.
Установка и изменение значения Y или D в столбце Recommended выполняется по процедуре IETF Standards Action с рецензией экспертов или по процедуре IESG Approval [RFC8126].
- Добавлена ссылка на данный документ.
- В реестр TLS HashAlgorithm добавлен столбец Recommended, как показано ниже.

Таблица 4.

Значение	Описание	Рекомендовано
0	none	Y
1	md5	D
2	sha1	D
3	sha224	D
4	sha256	Y
5	sha384	Y
6	sha512	Y
8	Intrinsic	Y

- Добавлено примечание к столбцу Recommended в соответствии с параграфом 3.1.

10. Реестр алгоритмов подписи TLS

TLS 1.0 и TLS 1.1 признаны устаревшими [RFC8996], TLS 1.2 будет применяться ещё некоторое время. В соответствии с изменением для столбца Recommended агентство IANA обновило реестр TLS SignatureAlgorithm.

- Обновлена процедура регистрации.
Установка и изменение значения Y или D в столбце Recommended выполняется по процедуре IETF Standards Action с рецензией экспертов или по процедуре IESG Approval [RFC8126].
- Добавлена ссылка на данный документ.

- В реестр TLS SignatureAlgorithm добавлен столбец Recommended, как показано ниже.

Таблица 5.

Значение	Описание	Рекомендовано
0	anonymous	N
1	rsa	Y
2	dsa	N
3	ecdsa	Y
7	ed25519	Y
8	ed448	Y
64	gostr34102012_256	N
65	gostr34102012_512	N

- Добавлено примечание к столбцу Recommended в соответствии с параграфом 3.1.

11. Реестр идентификаторов типа сертификата клиента TLS

TLS 1.0 и TLS 1.1 признаны устаревшими [RFC8996], TLS 1.2 будет применяться ещё некоторое время. В соответствии с изменением для столбца Recommended агентство IANA обновило реестр TLS ClientCertificateType Identifiers.

- Обновлена процедура регистрации.
Установка и изменение значения Y или D в столбце Recommended выполняется по процедуре IETF Standards Action с рецензией экспертов или по процедуре IESG Approval [RFC8126].
- Добавлена ссылка на данный документ.
- В реестр TLS ClientCertificateType Identifiers добавлен столбец Recommended, как показано ниже.

Таблица 6.

Значение	Описание	Рекомендовано
1	rsa_sign	Y
2	dss_sign	N
3	rsa_fixed_dh	N
4	dss_fixed_dh	N
5	rsa_ephemeral_dh_RESERVED	D
6	dss_ephemeral_dh_RESERVED	D
20	fortezza_dms_RESERVED	D
64	ecdsa_sign	Y
65	rsa_fixed_ecdh	N
66	ecdsa_fixed_ecdh	N
67	gost_sign256	N
68	gost_sign512	N

- Добавлено примечание к столбцу Recommended в соответствии с параграфом 3.1.

12. Реестр режимов обмена ключами TLS PskKeyExchangeMode

В соответствии с изменением для столбца Recommended агентство IANA обновило реестр TLS PskKeyExchangeMode.

- Обновлена процедура регистрации.
Установка и изменение значения Y или D в столбце Recommended выполняется по процедуре IETF Standards Action с рецензией экспертов или по процедуре IESG Approval [RFC8126].
- Добавлена ссылка на данный документ.
- В записях со значениями Y и N столбец Recommended не изменён.
- Обновлено примечание к столбцу Recommended в соответствии с параграфом 3.1.

13. Реестр схем подписи TLS

В соответствии с изменением для столбца Recommended агентство IANA обновило реестр TLS SignatureScheme.

- Обновлена процедура регистрации.
Установка и изменение значения Y или D в столбце Recommended выполняется по процедуре IETF Standards Action с рецензией экспертов или по процедуре IESG Approval [RFC8126].
- Добавлена ссылка на данный документ.
- В записях со значениями Y и N столбец Recommended не изменён.
- Обновлено примечание к столбцу Recommended в соответствии с параграфом 3.1.

14. Добавление столбца Comment

Агентство IANA добавило столбец Comment в указанные ниже реестры.

- TLS ExtensionType Values
- TLS Application-Layer Protocol Negotiation (ALPN) Protocol IDs
- TLS CachedInformationType Values
- TLS Certificate Compression Algorithm IDs

- TLS ClientCertificateType Identifiers
- TLS Cipher Suites
- TLS ContentType
- TLS EC Point Formats
- TLS EC Curve Types
- TLS Supplemental Data Formats (SupplementalDataType)
- TLS UserMappingType Values
- TLS SignatureAlgorithm
- TLS HashAlgorithm
- TLS Authorization Data Formats
- TLS Heartbeat Message Types
- TLS Heartbeat Modes
- TLS SignatureScheme
- TLS PskKeyExchangeMode
- TLS KDF Identifiers
- TLS SSLKEYLOGFILE Labels

В этом списке приведены все реестры, где ещё не было столбца Comment или Note, не отменённые TLS 1.3.

15. Рецензия экспертов на документы IETF и IRTF

Выбор процедуры Specification Required для кодов TLS обусловлен желанием упростить регистрацию для кодов, связанных с протоколами и алгоритмами, которые активно не разрабатываются в рамках IETF или IRTF. Разработку технологий на базе TLS в рамках IETF или IRTF следует вести в координации с рабочей группой TLS для надлежащего рецензирования. По этой причине назначенным экспертам следует отклонять регистрацию кодов для документов, которые уже приняты или предлагаются к принятию рабочими группами IETF или исследовательскими группами IRTF, если председатель рабочей группы TLS не укажет иное по электронной почте.

16. Регистрационные запросы

Запросы на регистрацию **должны** подаваться одним из указанных ниже способов.

1. Отправки по адресу iana@iana.org; в поле subject **следует** указывать цель (например, Request to register value in TLS bar registry).
2. Путём заполнения формы на странице <https://www.iana.org/form/protocol-assignment>.

Запросы по процедуре Specification Required [RFC8126] регистрируются после трехнедельного рассмотрения по рекомендации одного или нескольких назначенных экспертов. Для обеспечения возможности выделения значений до публикации назначенные эксперты могут одобрить регистрацию, как только убедятся, что спецификация будет опубликована.

17. Вопросы безопасности

Рекомендуемые алгоритмы считаются безопасными для общего пользования на момент регистрации, однако со временем криптографические алгоритмы и параметры могут быть взломаны или сочтены слабыми. Возможно, что статус Recommended в реестре не будет соответствовать последним достижениям в сфере криптоанализа. Разработчикам и пользователям нужно проверять поддержку приведёнными в реестрах алгоритмами желаемого уровня безопасности.

Назначенные эксперты проверяют публичную доступность спецификации и могут представлять более глубокие обзоры. Такие обзоры не следует считать одобрением шифронаборов, расширений, поддерживаемых групп и т. п.

18. Взаимодействие с IANA

Этот документ целиком посвящён изменениям связанных с TLS реестров IANA.

19. 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>>.
- [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>>.
- [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>>.
- [RFC7465] Popov, A., "Prohibiting RC4 Cipher Suites", RFC 7465, DOI 10.17487/RFC7465, February 2015, <<https://www.rfc-editor.org/info/rfc7465>>.
- [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>>.
- [RFC8447] Salowey, J. and S. Turner, "IANA Registry Updates for TLS and DTLS", [RFC 8447](#), DOI 10.17487/RFC8447, August 2018, <<https://www.rfc-editor.org/info/rfc8447>>.
- [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>>.
- [RFC9155] Velvindron, L., Moriarty, K., and A. Ghedini, "Deprecating MD5 and SHA-1 Signature Hashes in TLS 1.2 and DTLS 1.2", [RFC 9155](#), DOI 10.17487/RFC9155, December 2021, <<https://www.rfc-editor.org/info/rfc9155>>.

Адреса авторов

Joe Salowey
CyberArk
Email: joe@salowey.net

Sean Turner
sn3rd
Email: sean@sn3rd.com

Перевод на русский язык

Николай Малых
nmalykh@protokols.ru