Network Working Group
Request for Comments: 4835
Obsoletes: 4305
Category: Standards Track

V. Manral
IP Infusion Inc.

April 2007

# Требования к реализациям криптографических алгоритмов для ESP и AH

**Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)**

**Статус документа**

Это документ содержит проект стандарта протокола Internet для сообщества Internet и служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации и статус протокола можно узнать из текущей версии документа Internet Official Protocol Standards (STD 1). Допускается свободное распространение документа.

**Авторские права**



**Аннотация**

Группа протоколов IPsec использует различные криптографические алгоритмы для обеспечения услуг защиты. Протоколы ESP[1] и AH[2]) обеспечивают два механизма защиты данных, передаваемых через IPsec SA[3]. Для обеспечения совместимости требуется задать набор обязательных для реализации алгоритмов, чтобы гарантировать поддержку всеми реализациями хотя одного алгоритма. В этом документе определяется набор обязательных для реализации в протоколах ESP и AH алгоритмов, а также указаны алгоритмы, которые следует реализовать, поскольку они могут быть отнесены в будущем к числу обязательных.

# Оглавление



## *1. Введение*

Протоколы ESP и AH обеспечивают два механизма для защиты данных, передаваемых через IPsec SA [RFC4301], [RFC4302]. Для обеспечения совместимости требуется задать набор обязательных для реализации алгоритмов, чтобы гарантировать поддержку всеми реализациями хотя одного алгоритма. В этом документе определяется набор обязательных для реализации в протоколах ESP и AH алгоритмов, а также указаны алгоритмы, которые следует реализовать, поскольку они могут быть отнесены в будущем к числу обязательных.

По самой природе криптографии пространство новых алгоритмов и существующие алгоритмы подвергаются непрерывным атакам. Алгоритмы, считающиеся достаточно сильными сегодня, могут завтра обнаружить свои уязвимости. С учётом этого выбирать обязательные для реализации алгоритмы следует достаточно консервативно чтобы снизить вероятность быстрой компрометации выбранных алгоритмов. Следует также принимать во внимание вопросы производительности, поскольку многие приложения IPsec будут использоваться в средах, где производительность важна.

Наконец, следует признать, что обязательные для реализации алгоритмы нужно менять время от времени с учётом происходящих в мире изменений. По этой причине выбор обязательных для реализации алгоритмов не включён в основные спецификации IPsec, ESP и AH. Вместо этого был создан настоящий документ. При смене алгоритмов достаточно будет обновить только один документ.

В идеальном случае алгоритмам, которые будут внесены в число обязательных для реализации завтра, уже следует присутствовать в большинстве реализаций IPsec на момент придания им статуса обязательных. Для облегчения этого мы будем пытаться идентифицировать такие алгоритмы (поскольку они уже известны) в данном документе. Не существует гарантий того, что указанные алгоритмы станут в будущем обязательными, но они могут ими стать. Все известные алгоритмы являются объектами атак и использование любого из них может быть прекращено в будущем.

[1]Encapsulating Security Payload - инкапсуляция защищённых данных.
[2]Authentication Header - заголовок аутентификации.
[3]Security Association - защищённая связь.

# 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), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с [RFC2119].

Кроме того, здесь определено несколько дополнительных уровней.

***SHOULD+***
Этот термин обозначает то же, что и SHOULD. Однако, алгоритм, помеченный как SHOULD+, в будущем перейдёт в число **обязательных** (MUST).

***SHOULD-***
Этот термин обозначает то же, что и SHOULD. Однако, алгоритм, помеченный как SHOULD-, может перейти на уровень **разрешённых** (MAY) или ниже в будущих версиях этого документа.

***MUST-***
Этот термин обозначает то же, что и MUST. Однако мы предполагаем, что в какой-то момент этот алгоритм перестанет быть **обязательным**.

# 3. Выбор алгоритма

Для обеспечения совместимости реализаций IPsec требуется поддержка по крайней мере одного общего алгоритма защиты. В этом разделе приведены требования по реализации алгоритмов защиты для соответствующих спецификации реализаций протоколов ESP и AH. Алгоритмы защиты, реально используемые любой конкретной защищённой связью ESP или AH, определяются механизмом согласования (таким, как IKE[1] [RFC2409], [RFC4306]) или задаются при организации соединения.

Естественно, допускается реализация дополнительных (стандартных или фирменных) алгоритмов, не упомянутых в этом документе.

## 3.1. Протокол ESP

Требования в поддержке алгоритмов защиты для соответствующих спецификации реализаций протокола ESP приведены ниже. Определения уровней требований (колонка Требования) содержатся в разделе 2.

### 3.1.1. Алгоритмы шифрования и аутентификации для ESP

В приведённых ниже таблицах указаны требования к алгоритмам шифрования и аутентификации для протокола IPsec ESP.

| **Требования** | **Алгоритм шифрования** |
|---|---|
| MUST - **обязательно** | NULL [RFC2410][2] |
| MUST - **обязательно** | AES-CBC со 128-битовыми ключами [RFC3602] |
| MUST- - **обязательно** , но может утратить статус | TripleDES-CBC [RFC2451] |
| SHOULD - **следует** | AES-CTR [RFC3686] |
| SHOULD NOT - **не следует** | DES-CBC [RFC2405][3] |

| **Требования** | **Алгоритм аутентификации** |
|---|---|
| MUST - **обязательно** | HMAC-SHA1-96 [RFC2404][4] |
| SHOULD+ - **следует**, но может стать обязательным | AES-XCBC-MAC-96 [RFC3566] |
| MAY - **возможно** | NULL[2] |
| MAY - **возможно** | HMAC-MD5-96 [RFC2403][5] |

### 3.1.2. Комбинированные алгоритмы для ESP

Как указано в [RFC4303], протокол поддерживает использование комбинированных алгоритмов, которые обеспечивают услуги конфиденциальности и аутентификации. Поддержка таких алгоритмов требует соответствующего структурирования реализации ESP. Во многих ситуациях комбинированные алгоритмы обеспечивают значительные преимущества в части эффективности и пропускной способности. Хотя в настоящее время не указывается предлагаемых или обязательных к реализации комбинированных алгоритмов, предполагается, что в ближайшем будущем представят интерес алгоритмы AES-CCM [RFC4309] и AES-GCM [RFC4106]. Алгоритм AES-CCM принят в качестве предпочтительного для IEEE 802.11 [802.11i], а AES- GCM - для IEEE 802.1ae [802.1ae].

## 3.2. Протокол AH

Ниже приведены требования к реализации алгоритмов защиты в соответствующих спецификации реализациях протокола AH. Определения уровней требований (колонка Требования) приведены в разделе 2. Как вы понимаете, все перечисленные алгоритмы относятся к числу алгоритмов аутентификации.

| **Требования** | **Алгоритм аутентификации** |
|---|---|
| MUST - **обязательно** | HMAC-SHA1-96 [RFC2404][6] |
| SHOULD+ - **следует**, но может стать обязательным | AES-XCBC-MAC-96 [RFC3566] |
| MAY - **возможно** | HMAC-MD5-96 [RFC2403][7] |

[1]Internet Key Exchange — обмен ключами в Internet.
[2]Поскольку шифрование в ESP является необязательными, поддержка алгоритма NULL требуется для обеспечения совместимости со способом согласования услуг. Отметим, что, несмотря на возможность использования алгоритма NULL и для аутентификации, **недопустимо** использование NULL для обоих алгоритмов сразу [RFC4301].
[3]Алгоритм DES с его малым размером ключей и публично показанной открытой аппаратурой для взлома, является сомнительным средством защиты общего пользования.
[4]В алгоритме SHA-1 проявились слабые стороны [SHA1-COLL], однако это не должно влиять на использование SHA1 с HMAC.
[5]В алгоритме MD5 проявились слабые стороны [MD5-COLL], однако это не должно влиять на использование MD5 с HMAC.
[6]В алгоритме SHA-1 проявились слабые стороны [SHA1-COLL], однако это не должно влиять на использование SHA1 с HMAC.
[7]В алгоритме MD5 проявились слабые стороны [MD5-COLL], однако это не должно влиять на использование MD5 с HMAC.

# 4. Вопросы безопасности

Безопасность криптографически защищённых систем зависит от стойкости выбранных криптографических алгоритмов и используемых этими алгоритмами ключей. Кроме того, безопасность зависит также от устройства и администрирования протокола, используемого для предотвращения обхода криптосистемы.

Этот документ посвящён выбору криптографических алгоритмов для использования с протоколами ESP и AH и, в частности, обязательных для реализации алгоритмов. Алгоритмы, которые в соответствии с этой спецификацией **требуется** (MUST) или **следует** (SHOULD) реализовать, не имеют в данный момент известных фактов взлома и выполненные криптографические исследования позволяют надеяться, что эти алгоритмы останутся безопасными в обозримом будущем. Однако, такое положение дел не обязательно сохранится. Мы, следовательно, предполагаем появление новых версий этого документа, отражающих накопленный в сфере защиты опыт.

# 5. Благодарности

Значительная часть этого документа перенесена из RFC 4305, являющегося предшественником данного документа. Сам RFC 4305 заимствует часть текста из документа Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 [RFC4307], подготовленного Jeffrey I. Schiller.

Спасибо перечисленным здесь людям, которые указали ошибки в RFC 4305 или ответили на сообщения об их обнаружении: Paul Hoffman, Stephen Kent, Paul Koning и Lars Volker. Полезные комментарии были получены от Russ Housley, Elwyn Davies, Nicolas Williams и Alfred Hoenes.

# 6. Отличия RFC 2402 и RFC 2406 от RFC 4305

[RFC2402] и [RFC2406] определяли протоколы IPsec AH и IPsec ESP. Каждый из этих документов содержал требования к криптографическим алгоритмам для соответствующего протокола. В настоящее время эти спецификации заменены документами [RFC4302] и [RFC4303], которые не содержат требований к реализации криптографических алгоритмов. В данном документе указаны такие требования для обоих протоколов - [RFC4302] и [RFC4303].

Сравнение требований приведено ниже.

| Старое требование | Старый RFC | Новое требование | Алгоритм |
|---|---|---|---|
| MUST - **требуется** | 2406 | SHOULD NOT - **не следует** | DES-CBC [RFC2405][1] |
| MUST - **требуется** | 2402, 2406 | MAY - **возможно** | HMAC-MD5-96 [RFC2403] |
| MUST - **требуется** | 2402, 2406 | MUST - **требуется** | HMAC-SHA1-96 [RFC2404] |

# 7. Отличия от RFC 4305

Этот документ является заменой [RFC4305]. Документ меняет требование по поддержке алгоритма аутентификации NULL с MUST (**требуется**) на MAY (**возможно**). Это изменение внесено для обеспечения согласованности с [RFC4301]. Добавлен текст об атаках с использованием конфликтов SHA-1, а также отмечены, как предполагаемые для использования в будущем, алгоритмы AES-GCM и AES-CCM.

Изменённые требования к поддержке алгоритмов в реализациях протоколов перечислены в таблице.

| Старое требование | Старый RFC | Новое требование | Алгоритм |
|---|---|---|---|
| MUST - **требуется** | 2406 | MAY - **возможно** | Аутентификация NULL |
| MUST - **требуется** | 2406 | MUST **- требуется** | Шифрование NULL |
| SHOULD+ - **следует** с возможностью перехода в **должно** | 4305 | MUST - **требуется** | Шифрование AES-CBC |

# 8. Литература

## 8.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP14, RFC2119, March 1997.

[RFC2403] Madson, C. and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", RFC 2403, November 1998.

[RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.

[RFC2405] Madson, C. and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, November 1998.

[RFC2410] Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.

[RFC2451] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

[RFC3566] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.

[RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.

[RFC3686] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[1] IETF запрещает самостоятельное использование DES уже много лет и не включает этот алгоритм в новые стандарты в течение достаточного времени (см. комментарий IESG на первой странице [RFC2407]). [RFC4305] является первым проектом стандарта, в котором указано, что реализациям **не следует** использовать алгоритм DES самостоятельно (не в комбинации с другими, *прим. перев.)*. Институт стандартов и технологий США (NIST) формально признал слабость DES при самостоятельном использовании в документе [DES-WDRAW], призывая прекратить использование этого алгоритма в качестве Государственного стандарта США. Алгоритм Triple DES по прежнему признается как IETF, так и NIST.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4305] Eastlake, D., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4305, December 2005.

## 8.2. Дополнительная литература

[802.11i] "LAN/MAN Specific Requirements Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications", IEEE Standard Medium Access Control (MAC) Security, IEEE Std 802.11i, June 2004.

[802.1ae] "Media Access Control (MAC) Security", IEEE Standard Medium Access Control (MAC) Security, IEEE Std 802.1ae, June 2006.

[DES-WDRAW] "Announcing Proposed Withdrawal of Federal Information Processing Standard (FIPS) for the Data Encryption Standard (DES) and Request for Comments", FIPS Notice Docket No. 040602169-4169-01, July 2004.

[MD5-COLL] Klima, V., "Finding MD5 Collisions - a Toy For a Notebook", Cryptology ePrint Archive Medium Report 2005/075, March 2005.

[RFC2402] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC 4106, June 2005.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4307] Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", RFC 4307, December 2005.

[RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.

[SHA1-COLL] Rijmen, V. and E. Oswald, "Update on SHA-1", Cryptology ePrint Archive Report 2005/010, January 2005.

### Адрес автора

**Vishwas Manral**
IP Infusion Inc.
Bamankhola, Bansgali,
Almora, Uttarakhand 263601
India
Phone: +91-98456-61911
EMail: vishwas@ipinfusion.com

### Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

### Полное заявление авторских прав



### Интеллектуальная собственность

IETF предлагает любой заинтересованной стороне обратить внимание на авторские права, патенты или использование патентов, а также иные права собственности, которые могут потребоваться для реализации этого стандарта. Информацию следует направлять в IETF по адресу ietf-ipr@ietf.org.

**Подтверждение**

Финансирование функций RFC Editor обеспечено IETF Administrative Support Activity (IASA).