ТК26, рабочая группа IPsec
Предварительный документ
<rus-fedchenko-cpah-ipsecme-gost-00-rk>
Предполагаемый статус: Информационный
Действителен: Август 2010

С.Е. Леонтьев, Editor
М.В. Павлов, Editor
CRYPTO-PRO
А.А. Федченко, Editor
S-Terra
December 2009

Алгоритмы обеспечения целостности IPsec (ESP, AH) на основе ГОСТ Р 34.11-94

rus-fedchenko-cpah-ipsecme-gost-00-rk

Статус документа

[TODO: а надо ли в документе ТК26 авторам предоставлять права, и если надо, то как именно?]

Фактом передачи предварительного документа в ТК26, каждый автор соглашается с неэксклюзивным предоставлением IPR для ТК26, аналогично положениям стандарта Интернет IETF BCP 79.

Данный предварительный документ является открытым документом "Рабочей группы IPsec и IKE", "Технического комитета по стандартизации "Криптографическая защита информации" (ТК26). Область распространения документа не ограничена.

Данный предварительный документ действителен в течении максимум девяти месяцев, и может быть в любое время изменён, заменён на другой или отозван в любое время. При цитировании или ссылке на него из других документов следует ставить отметку, что “документ готовится к публикации”.

Список предварительных документов ТК26 доступен по <http://www.tc26.ru/>.

Этот предварительный документ действителен до Август 2010.

Аннотация

Это предварительный документ на русском языке предназначен для обеспечения совместимости реализаций IPsec AH российских производителей, а так же для создания проекта документа IETF.

Этот документ описывает соглашения по использованию ГОСТ Р 34.11-94 для обеспечения целостности (Integrity Algorithm) вложений IPsec ESP и пакетов IPsec AH. Протокол ESP используется для обеспечения конфиденциальности (опционально), целостности и аутентичности содержимого IP пакетов. Протокол AH используется для обеспечения целостности и аутентичности IP пакетов (вместе с заголовком).

Лист изменений

Предназначено для подготовки I-D и его поддержки. Убрать в момент публикации RFC.

00-ra 2008-07-26 ЛСЕ	"Рыба", только оглавление и ссылки;
00-rb 2008-08-14 ЛСЕ	Терминология ESP;

00-rc 2009-02-15 ЛСЕ	Выделил Integrity Algorithm ESP и AH в отдельный документ; Упомянул внутреннее выравнивание ГОСТ Р 34.11-94, описанное в стандарте;
00-rd 2009-03-01 ЛСЕ	Описание PDF, XML Validated; Подготовлено для согласования с Владимиром Олеговичем Поповым.
00-re 2009-03-16 ЛСЕ	Удалено описание ICVCounter, оно не нужно, т.к. ключ HMAC меняется, либо каждые 4 Мбайт, либо каждый пакет; Термин "неаутентифицированный пакет" заменён на термин "искажённый пакет"; Исправлены нестандартные по [KEYWORDS] термины; Документ, который должен вводить идентификатор ГОСТ Р 34.11-94 для [IKE] пока под вопросом.
00-rf 2009-03-16 ЛСЕ	Удалены метки конфиденциальности и Copyright; Добавлены рыбы тестовых примеров; Вставлены окончательные значения примеров хэш-функции; Вставлен редактор английского перевода;
00-rg 2009-12-02 ПВО & ЛСЕ	Убрано описание хэш-функции ГОСТ Р 34.11-94, перенесено в [draft.CPIKE], т.к. в основном хэш-функция используется там. Замечу, что [draft.CPIKE] - обзателен к реализации, а этот документ - нет; Внесено описание опционального алгоритма "Использование совместно с алгоритмами обеспечения целостности IPsec ГОСТ Р 34.11-94", перенесено из [draft.CPESP], т.к. это позволило убрать "паразитную" ссылку между документами, а для основных применений IPsec [ESP] (КС1-КС3) этот алгоритм без надобности; Теперь только этот документ содержит нормативные ссылки на предварительные документы [draft.CPIKE] и [draft.CPESP]. И это хорошо, т.к. данный документ посвящён опциональным алгоритмам, а те посвящены обязательным алгоритмам.
00-rh 2009-12-07 ЛСЕ	Учтены остальные замечания Смыслова Валерия Анатольевича, ОАО "ЭЛВИС-ПЛЮС".
00-ri 2009-12-08 ПВО & ЛСЕ	Исправлены примеры.
00-rk 2010-07-15 ЛСЕ	Учтены замечания Мартанова Георгия Олеговича, НТЦ "Атлас" и Смыслова Валерия Анатольевича, ОАО "ЭЛВИС-ПЛЮС" об исключении специального случая использования HMAC для решений КВ и выше.

Авторские замечание

Предназначено для подготовки I-D и его поддержки. Убрать в момент публикации RFC.

Описание формата проекта RFC в XML (Internet-Draft или I-D), методы просмотра, форматирования и редактирования смотри [draft.RFC2629bis] [RFC2629] [XML2RFC] [ID-Checklist] [xml2rfc-validator]

Текущий регистр [DOI] <http://www.iana.org/assignments/isakmp-registry> [isakmp-registry]

Текущий регистр [IKE] <http://www.iana.org/assignments/ipsec-registry> [ipsec-registry]

Должен нормально просматриваться в любом достаточно современном browser-е при активном подключении к сети Интернет.

Извините за язык "падонков", но используем шаблон [XML2RFC] на английском языке, хотя и пишем по-русски.

При преобразовании в PDF следует настроить FO процессор на использование встраиваемых русских шрифтов, см. Кратчайший путь к DocBook [1].

В документе используются применяемые в IETF расширения " Draft HTML and PDF from XML source [2]", поэтому после перевода на английский надо будет применять XSLT преобразование "xml2rfc\rfc2629xslt\clean-for-DTD.xslt" перед вызовом "xml2rfc\xml2rfc.tcl" для получения текстового файла.

[1] http://docbook.ru/doc/sw/foproc.html
[2] http://greenbytes.de/tech/webdav/rfc2629xslt/rfc2629xslt.html

Содержание

1. Введение

Данный документ определяет следующие преобразования [AH] и алгоритмы обеспечения целостности [ESP]:

- AH_GOST-HMAC-4M и GOST-HMAC-4M;
- AH_GOST-HMAC-1K и GOST-HMAC-1K;

Протоколы [AH] и [ESP] используется в архитектуре IPsec [ARCH] для обеспечения конфиденциальности, целостности и аутентичности содержимого IP пакетов. Этот документ описывает использование ГОСТ Р 34.11-94 [GOST3431195] [GOSTR341194] в AH и ESP, но не определяет сами алгоритмы и форматы представления криптографических типов данных. Алгоритмы описываются соответствующими национальными стандартами, а представление данных и параметров соответствует следующими документам IETF [CPALGS] [CPPK] [CPCMS] и [draft.CPIKE].

AH пакеты и ESP вложения обрабатываются в рамках IPsec SA, параметры которой MAY интерпретироваться согласно [DOI]. Этот документ описывает так же дополнительные идентификаторы расширяющие [DOI].

2. Терминология

Термины "ДОЛЖНО", "ДОЛЖНА", "ДОЛЖНЫ", "ДОЛЖЕН" (MUST, REQUIRED, SHALL), "НЕ ДОЛЖЕН", "НЕ ДОЛЖНЫ" (MUST NOT, SHALL NOT), "РЕКОМЕНДОВАНО" (SHOULD, RECOMMENDED), "НЕ РЕКОМЕНДОВАНО" (SHOULD NOT, NOT RECOMMENDED), "МОГУТ", "МОЖЕТ" (MAY, OPTIONAL) в рамках этого документа ДОЛЖНЫ интерпретироваться в соответствии с RFC 2119 [KEYWORDS].

В документе используются термины и определения стандартов IPsec [ARCH], [ESP] и [AH], ниже приводятся только дополнительные определения.

Divers(K,D):	алгоритм диверсификации ключа K по данным D (Section 7 of [CPALGS]). Узел замены определяется Раздел 6. В целях настоящего документа, аргументом D является 64-битное целое число, представленное в сетевом порядке байт;
HMAC_GOSTR3411(K, text):	выработка HMAC ГОСТ Р 34.11-94 на ключе K от данных text с внутренним выравниванием по ГОСТ Р 34.11-94 (Section 3 of [CPALGS], описание и пример сетевого представления результата ГОСТ Р 34.11-94 приведён в Section 2.1 of [CPCMS]);
Ki_i(Seq#):	ключ алгоритма имитозащиты пакета Seq#;
Kr_i:	корневой ключ имитозащиты SA;
Seq#:	64-битный номер пакета, если [ESN] не согласован, то значение Seq# всегда принадлежит диапазону 1..2^32-1;
Seq#h:	старшая часть Seq#;
Seq#l:	младшая часть Seq#;
substr(s..f, bytes):	последовательность байт с байта s, по байт f, выбранная из представленной в сетевом порядке последовательности bytes;
bits[s..f]:	последовательность бит с бита s, по бит f, выбранная из представленной в сетевом порядке последовательности bits;
пакет с искажённым Seq#:	ESP вложение или AH пакет для которого не прошёл предварительный контроль SPI и Seq#;
искажённый пакет:	ESP вложение или AH пакет для которого вычисленное значение ICV не совпало с переданным значением;

3. Состав AH_GOST SA

В рамках ISAKMP SA [draft.CPIKE] или иной не-IPsec SA согласуются для данной IPsec SA, как минимум, следующие компоненты:

- 256-бит симметричный ключ Kr_i (используется K1);
- параметры ГОСТ 28147-89;
- максимальный объём данных SA в байтах (Lifetime SA, Kbytes);
- максимальный время жизни SA в секундах (Lifetime SA, sec);
- максимальное значение счётчика искажённых пакетов.

4. Преобразования

Заголовок AH пакета ДОЛЖЕН соответствовать Section 2 of [AH] со следующими параметрами:

- Явного выравнивания ICV не производится;
- ICV имеет размер 12 байт.

Для SA ДОЛЖНА быть включена услуга обеспечения защиты от навязывания повторных пакетов (anti-replay).

Для преобразования AH_GOST-HMAC-4M используется алгоритм GOST-HMAC-4M, для преобразования AH_GOST-HMAC-1K используется алгоритм GOST-HMAC-1K.

5. Алгоритмы обеспечения целостности ГОСТ Р 34.11-94

Алгоритмы GOST-HMAC-4M() и GOST-HMAC-1K() предназначены для обеспечения целостности вложений [ESP] при применении с различными алгоритмами шифрования вложений. Основным применением данных алгоритмов является совместная работа с преобразованием ESP_NULL, т.е. услуга целостности вложения без услуги конфиденциальности.

Для SA ДОЛЖНА быть включена услуга обеспечения защиты от навязывания повторных пакетов (anti-replay).

Результатом алгоритмов GOST-HMAC-4M() и GOST-HMAC-1K() является значение ICV, которое имеет следующий вид:

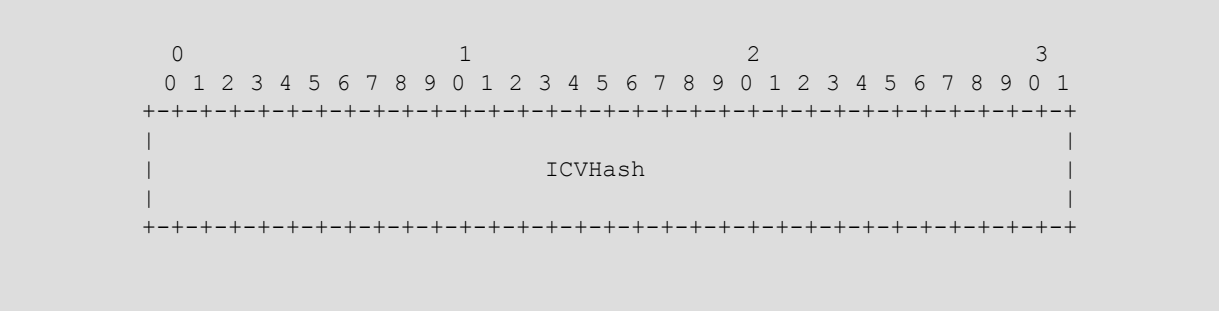

Figure 1: ICV для GOST-HMAC-4M и GOST-HMAC-1K

, где

h = HMAC_GOSTR3411(Ki_e(Seq#), Data);

,где HMAC_GOSTR3411() описан Section 3 of [CPALGS], описание и пример сетевого представления результата ГОСТ Р 34.11-94 дано в Section 2.1 of [CPCMS]

ICVHash = substr(0..11, h);

5.1 Обработка исходящих пакетов

Порядок обработки исходящих пакетов ДОЛЖЕН соответствовать Section 3.3 of [AH], Section 3.3 of [ESP] со следующими уточнениями:

- Дополнительно к проверкам Section 3.3.1 of [AH] и Section 3.3.1 of [ESP] РЕКОМЕНДОВАНО проверить длину IP пакета на соответствие параметрам SA; [rfc.comment.1]
- ICV в преобразованиях вырабатывается для AH_GOST-HMAC-4M по формуле:

  ICV = GOST-HMAC-4M(Ki_e(Seq#), IPhdr|..[|Seq#h])

  , а для AH_GOST-HMAC-1K

  ICV = GOST-HMAC-1K(Ki_e(Seq#), IPhdr|..[|Seq#h])

  [rfc.comment.2]
- Отправителю РЕКОМЕНДОВАНО увеличить счётчик текущего объём данных SA в байтах (Lifetime SA, Kbytes) и сравнить его с максимальным. При его превышении РЕКОМЕНДОВАНО заблокировать дальнейшую работу SA. [rfc.comment.3]

[rfc.comment.1] Аудит - "No valid Security Association exists"

[rfc.comment.2] Аудит - "Attempt to transmit a packet that would result in Sequence Number overflow"

[rfc.comment.3] Аудит - "Attempt to transmit a packet that would result in Sequence Number overflow"

5.2 Обработка входящих пакетов

Порядок обработки входящих пакетов ДОЛЖЕН соответствовать Section 3.4 of [AH] Section 3.4 of [ESP] со следующими уточнениями:

- Дополнительно к проверкам Section 3.4.2 of [AH] Section 3.4.2 of [ESP], РЕКОМЕНДОВАНО проверить длину IP пакета на соответствие параметрам SA; [rfc.comment.4]
- Получателю РЕКОМЕНДОВАНО увеличить счётчик текущего объём данных SA в байтах (Lifetime SA, Kbytes) и сравнить его с максимальным. SA в байтах (Lifetime SA, Kbytes) и сравнить его с максимальным. При его превышении РЕКОМЕНДОВАНО заблокировать дальнейшую работу SA; [rfc.comment.5]
- ICV в преобразованиях проверяется для AH_GOST-HMAC-4M по формуле:

  ICVchk = GOST-HMAC-4M(Ki_i(Seq#), IPhdr|..[|Seq#h])

  , а для AH_GOST-HMAC-1K

  ICVchk = GOST-HMAC-1K(Ki_i(Seq#), IPhdr|..[|Seq#h])
- Если ICV != ICVchk, то получателю РЕКОМЕНДОВАНО увеличить счётчик искажённых пакетов SA и сравнить его с максимальным. При его превышении РЕКОМЕНДОВАНО заблокировать дальнейшую работу SA; [rfc.comment.6]

5.3 Вычисление MTU

При вычислении MTU следует руководствоваться правилами Section 2 of [AH] и Section 2 of [ESP] с учётом фиксированного размера ICV - 12 байт, без выравнивания.

5.4 Алгоритм GOST-HMAC-4M

В алгоритме GOST-HMAC-4M используются:

```
Ki_i(Seq#) = Divers(Divers(Divers(Kr_i, Seq# & 0xffffffff00000000),
                Seq#&0xfffffffffff0000),
                Seq#&0xffffffffffffc0);
```

НЕ РЕКОМЕНДОВАНО согласовывать размеры AH пакетов (ESP вложений) более, чем 64 Кбайт.

5.5 Алгоритм GOST-HMAC-1K

В алгоритме GOST-HMAC-1K используются:

```
Ki_i(Seq#) = Divers(Divers(Divers(Kr_i, Seq#&0xffffffff00000000),
                Seq#&0xfffffffffff0000),
                Seq#);
```

[rfc.comment.4] Аудит - "No valid Security Association exists"

[rfc.comment.5] Аудит - "The received packet fails the anti-replay checks"

[rfc.comment.6] Аудит - "No valid Security Association exists"

6. Дополнительные параметры и атрибуты SA

Порядок согласования атрибутов описан Section 6 of [draft.CPESP]. Значения параметров по-умолчанию для AH_GOST-HMAC-4M, AH_GOST-HMAC-1K, GOST-HMAC-4M и GOST-HMAC-1K:

Параметр	**Атрибут**	**Формат**	**Умолчание**
Максимальное значение счётчика искажённых пакетов	32402	B	10^9
Максимальный размер пакета	32507	B	65536

Table 1: Параметры AH_GOST SA

7. Благодарности

Добрые слова в адрес российских CISCO, CheckPoint и Газпром...-а, который(е) инициировали попытку достижения совместимости...

Выражаем благодарность Чмора Андрею Львовичу, ОАО "Инфотекс", за дискуссию по определению понятия DoS.

Выражаем особую благодарность Смыслову Валерию Анатольевичу, ОАО "ЭЛВИС-ПЛЮС", за большое количество ценных замечаний и улучшений, как в сам протокол, так и в его описание.

Благодарности рецензентам, надеюсь такие найдутся...

8. Авторский коллектив

Адреса авторов


```
Дмитрий Г. Дьяченко
ООО Крипто-Про
Сущёвский вал., д. 16, стр. 5
Москва, 127018
Россия
Phone: +7 (495) 780 48 20
Fax: +7 (495) 780 48 20
EMail: lse@cryptopro.ru
URI: http://www.CryptoPro.ru

Владимир О. Попов
ООО Крипто-Про
Сущёвский вал., д. 16, стр. 5
Москва, 127018
Россия
Phone: +7 (495) 780 48 20
Fax: +7 (495) 780 48 20
EMail: lse@cryptopro.ru
URI: http://www.CryptoPro.ru

Кирилл А. Корнилов
S-Terra
Зеленоград, МГИЭТ, корпус 10, офис 110
Москва, 124498
Россия
Phone: +7 (495) 726 98 91
Fax: +7 (495) 531 9789
EMail: hell@s-terra.com
URI: http://www.s-terra.ru
```

9. Регистрация IANA

IANA выделяет два номера преобразований AH (ESP Authentication Algorithm) для использования ГОСТ Р 34.11-94:

<TBD-5> для AH_GOST-HMAC-4M и GOST-HMAC-4M;

<TBD-6> для AH_GOST-HMAC-1K и GOST-HMAC-1K.

9.1 Удалить после регистрации в IANA

Пока, предварительные реализации используют следующие приватные номера преобразований:

251 для AH_GOST-HMAC-4M и GOST-HMAC-4M;

250 для AH_GOST-HMAC-1K и GOST-HMAC-1K.

10. Обсуждение требований по безопасности

Параметры криптографических алгоритмов влияют на стойкость. Использование параметров, которые не перечислены в [CPALGS], НЕ РЕКОМЕНДОВАНО без соответствующих исследований Section 9 of [CPALGS].

Приложения РЕКОМЕНДОВАНО исследовать установленным порядком на соответствие заданным требованиям согласно [RFLLIC], и [CRYPTOLIC].

Приложениям РЕКОМЕНДОВАНО согласовывать время жизни SA (Lifetime SA), как по времени, так и по объёму переданной информации Section 4.4.2.1 of [ARCH]. НЕ РЕКОМЕНДОВАНО согласовывать время жизни SA (Lifetime SA) в секундах более, чем на 86400 сек (1 сутки).

НЕ РЕКОМЕНДОВАНО согласовывать время жизни SA в байтах (Lifetime SA, sec) более, чем на 2^80 байт.

НЕ РЕКОМЕНДОВАНО согласовывать параметр Max-Auth-Error больший чем 10^9, без соответствующего исследования.

Для приложений с требованиями по уровню защиты KB1 и выше НЕ РЕКОМЕНДОВАНО согласовывать параметр Max-Auth-Error больший чем 10^6, без соответствующего исследования.

11. Примеры

Представление данных в примере:

0xNNNN:	Представление целого числа в шестнадцатеричной системе счисления;
0xFFFFFFFF FF...:	Представление объктов в форме big-endian;
BBBBBBBB BB:	Представление в сетевой нотации. Числа в big-endian. Сетевое представление сложных объектов согласно стандартам их определяющих, в частности, ключей и хэшей согласно [CPALGS], [CPCMS] и [CPPK] [rfc.comment.7].

11.1 Тестовый пакет ESP_NULL+GOST-HMAC-4M

Открытые данные пакета, длина 53:

```
4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
20212223 24252627 28292a2b 2c2d2e2f 30313233 34
```

Параметры SA с алгоритмом шифрования ESP_NULL и алгоритмом обеспечения целостности GOST-HMAC-4M

```
   SPI
      31323334
   ECN
      несогласован
   Kr_e
      не используется данным алгоритмом
  Kr_i 0x
c00341ab 7f7fcbf1 65685590 76d601ce de8443ad 3c4264f2 0d71612d 7f1a4ecb
```

Промежуточные данные GOST-HMAC-4M

```
   Seq#l
      0x3d
  Kr_i2 = Divers(Kr_i, Seq# & 0xffffffff00000000) 0x
bddcedc2 c909edc4 14996cd1 705016e9 d050f04f 4fcbf179 1c82db23 aa388fe8
  Kr_i1 = Divers(Kr_i2, Seq# & 0xffffffffffff0000) 0x
f6519e6a 69b5ffb2 ece16f80 1d68ff14 8221028f c012863e 26d42296 ea7ca9bf
  Kc_i = Divers(Kr_i1, Seq# & 0xfffffffffffffffc0) 0x
7227fdb7 eb30f035 357aace7 e9009655 f0aa5e04 a2337279 4492f9f1 8ab27155
   Pad
      000104
   Seq#h
      не используется, т.к. ECN несогласован
   ICVpad
      не используется этим алгоритмом
   ICV
      d305bd80 1e385386 e17edfe8
```

[rfc.comment.7] Рабочее название "little-endian", хотя это и не совсем так.

ESP вложение длина 76 (== 8+53+3+12):

```
31323334 0000003d 4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617
18191a1b 1c1d1e1f 20212223 24252627 28292a2b 2c2d2e2f 30313233 34000104
d305bd80 1e385386 e17edfe8
```

11.2 Тестовый пакет ESP_NULL+GOST-HMAC-1K

Открытые данные пакета, длина 53:

```
4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f
20212223 24252627 28292a2b 2c2d2e2f 30313233 34
```

Параметры SA с алгоритмом шифрования ESP_NULL и алгоритмом обеспечения целостности GOST-HMAC-4M

```
   SPI
      31323334
   ECN
      несогласован
   Kr_e
      не используется данным алгоритмом
   Kr_i 0x
c00341ab 7f7fcbf1 65685590 76d601ce de8443ad 3c4264f2 0d71612d 7f1a4ecb
```

Промежуточные данные GOST-HMAC-4M

```
   Seq#l
      0x3d
  Kr_i2 = Divers(Kr_i, Seq# & 0xffffffff00000000) 0x
bddcedc2 c909edc4 14996cd1 705016e9 d050f04f 4fcbf179 1c82db23 aa388fe8
  Kr_i1 = Divers(Kr_i2, Seq# & 0xffffffffffff0000) 0x
f6519e6a 69b5ffb2 ece16f80 1d68ff14 8221028f c012863e 26d42296 ea7ca9bf
  Kc_i = Divers(Kr_i1, Seq#) 0x
7227fdb7 eb30f035 357aace7 e9009655 f0aa5e04 a2337279 4492f9f1 8ab27155

   Pad
      000104
   Seq#h
      не используется, т.к. ECN несогласован
   ICVpad
      не используется этим алгоритмом
   ICV
      d305bd80 1e385386 e17edfe8
```

ESP вложение длина 76 (== 8+53+3+12):

```
31323334 0000003d 4500001d 04050607 08090a0b 0c0d0e0f 10111213 14151617
18191a1b 1c1d1e1f 20212223 24252627 28292a2b 2c2d2e2f 30313233 34000104
d305bd80 1e385386 e17edfe8
```

11.3 Тестовый пакет AH GOST-HMAC-4M

Входной пакет с обнулёнными изменяемыми полями [AH] и вставленным заголовком AH, длина 84:

```
    vvvv Len        vv Protocol=51=AH        vv Next Header=01=ICMP
45000054 0a2c0000 00330000 c0a855a8 c0a85570 01040000 31323334 00000001
00000000 00000000 00000000 00005547 00010014 08090a0b 0c0d0e0f 10111213
14151617 18191a1b 1c1d1e1f 20212223 24252627
```

Параметры AH SA GOST-HMAC-1K

```
   SPI
      31323334
   ECN
      несогласован
   Kr_i 0x
9b6a7fda 8d484a43 f9e6ca9b b5a4acc5 be4015a2 c3c8c63d 88c9180b 911e3416
```

Промежуточные данные GOST-HMAC-4M

```
   Seq#l
      0x01
   Kr_i2 = Divers(Kr_i, Seq# & 0xffffffff00000000) 0x
d30906a9 e406a326 055499f4 8a252188 89035074 9bb311f8 0ad89e82 272106b1
  Kr_i1 = Divers(Kr_i2, Seq# & 0xffffffffffff0000) 0x
42b7e3d7 29ed8c75 9d55fac8 e77da973 d16ef39e 918d8944 d4f1a011 2a4a2214
  Kc_i = Divers(Kr_i1, Seq# & 0xfffffffffffffffc0) 0x
977f5345 eb1cd379 cbd38a96 cf2b51e1 198b7ad0 8d87761f 475a07e1 0699318b
   Seq#h
      не используется, т.к. ECN несогласован
   ICVpad
      не используется этим алгоритмом
   ICV
      e05d4ac4 f1c74bca 9c5fab29
```

AH пакет, длина 84:

```
      vvvv Len        vv Protocol=51=AH        vv Next Header=01=ICMP
 45000054 0a2c0000 00330000 c0a855a8 c0a85570 01040000 31323334 00000001
 e05d4ac4 f1c74bca 9c5fab29 00005547 00010014 08090a0b 0c0d0e0f 10111213
 14151617 18191a1b 1c1d1e1f 20212223 24252627
```

11.4 Тестовый пакет AH GOST-HMAC-1K

Входной пакет с обнулёнными изменяемыми полями [AH] и вставленным заголовком AH, длина 84:

```
    vvvv Len        vv Protocol=51=AH        vv Next Header=01=ICMP
 45000054 0a2c0000 00330000 c0a855a8 c0a85570 01040000 31323334 00000001
 00000000 00000000 00000000 00005547 00010014 08090a0b 0c0d0e0f 10111213
 14151617 18191a1b 1c1d1e1f 20212223 24252627
```

Параметры AH SA GOST-HMAC-1K

```
   SPI
      31323334
   ECN
      несогласован
   Kr_i 0x
9b6a7fda 8d484a43 f9e6ca9b b5a4acc5 be4015a2 c3c8c63d 88c9180b 911e3416
```

Промежуточные данные GOST-HMAC-1K

```
   Seq#1
      0x01
   Kr_i2 = Divers(Kr_i, Seq# & 0xffffffff00000000) 0x
d30906a9 e406a326 055499f4 8a252188 89035074 9bb311f8 0ad89e82 272106b1
  Kr_i1 = Divers(Kr_i2, Seq# & 0xffffffffffff0000) 0x
42b7e3d7 29ed8c75 9d55fac8 e77da973 d16ef39e 918d8944 d4f1a011 2a4a2214
  Kc_i = Divers(Kr_i1, Seq#) 0x
977f5345 eb1cd379 cbd38a96 cf2b51e1 198b7ad0 8d87761f 475a07e1 0699318b
   Seq#h
      не используется, т.к. ECN несогласован
   ICVpad
      не используется этим алгоритмом
   ICV
      e05d4ac4 f1c74bca 9c5fab29
```

AH пакет длина 84:

```
      vvvv Len        vv Protocol=51=AH       vv Next Header=01=ICMP
45000054 0a2c0000 00330000 c0a855a8 c0a85570 01040000 31323334 00000001
e05d4ac4 f1c74bca 9c5fab29 00005547 00010014 08090a0b 0c0d0e0f 10111213
14151617 18191a1b 1c1d1e1f 20212223 24252627
```

12. Библиография

12.1 Нормативные ссылки

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

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

[CPALGS] Popov, V., Kurepkin, I., and S. Leontiev, "Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms", RFC 4357, January 2006.

[CPCMS] Leontiev, S. and G. Chudov, "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)", RFC 4490, May 2006.

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

[draft.CPESP] Леонтьев, С.Е., Ed., Павлов, М.В., Ed., and А.А. Федченко, Ed., "Комбинированый алгоритмы шифрования вложений IPsec (ESP) на основе ГОСТ 28147-89", December 2009.

[draft.CPIKE] Леонтьев, С.Е., Ed., Павлов, М.В., Ed., and А.А. Федченко, Ed., "Использование ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при управлении ключами IKE и ISAKMP", December 2009.

[ESN] Kent, S., "Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)", RFC 4304, December 2005.

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

[GOST3431195] Council for Standardization, Metrology and Certification of the Commonwealth of Independence States (EASC), Minsk , "Information technology. Cryptographic Data Security. Cashing function (In Russian)", GOST 34.311-95, 1995.

[GOSTR341194] Government Committee of the Russia for Standards , "Information technology. Cryptographic Data Security. Hashing function, Gosudarstvennyi Standard of Russian Federation (In Russian)", GOST R 34.11-94, 1994.

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

[JUMBO] Borman, D., Deering, S., and R. Hinden, "IPv6 Jumbograms", RFC 2675, August 1999.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4134] Hoffman, P., "Examples of S/MIME Messages", RFC 4134, July 2005.

12.2 Информативные ссылки

[CPPK] Leontiev, S. and D. Shefanovski, "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 4491, May 2006.

[CRYPTOLIC] "Russian Federal Government Regulation on Licensing of Selected Activity Categories in Cryptography Area, 23 Sep 2002 N 691", September 2002.

[RFLLIC] "Russian Federal Law on Licensing of Selected Activity Categories, 08 Aug 2001 N 128-FZ", August 2001.

[Schneier95] Schnier, B., "Applied cryptography, second edition", John Wiley, 1995.

12.3 Библиотека ссылок

[AES-GMAC] McGrew, D. and J. Viega, "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", RFC 4543, May 2006.

[draft.CPAH] Леонтьев, С.Е., Ed., Павлов, М.В., Ed., and А.А. Федченко, Ed., "Алгоритмы обеспечения целостности IPsec (ESP, AH) на основе ГОСТ Р 34.11-94", December 2009.

[GOST28147] Government Committee of the USSR for Standards , "Cryptographic Protection for Data Processing System, Gosudarstvennyi Standard of USSR (In Russian)", GOST 28147-89, 1989.

[RFEDSL] "Russian Federal Electronic Digital Signature Law, 10 Jan 2002 N 1-FZ", January 2002.

12.4 Ссылки на примеры и методы редактирования

[draft.rfc2434bis] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", Internet-Draft draft-narten-iana-considerations-rfc2434bis-09 (work in progress), March 2008.

[draft.RFC2629bis] Rose, M.T., "Writing I-Ds and RFCs using XML (revised)", February 2009, <http://xml.resource.org/authoring/draft-mrose-writing-rfcs.html>.

[ID-Checklist] Wijnen, B., "Checklist for Internet-Drafts (IDs) submitted for RFC publication", October 2006, <http://www.ietf.org/ID-Checklist.html>.

[ipsec-registry] IANA, "Internet Key Exchange (IKE) Attributes - per RFC 2409 (IKE)", January 2009, <http://www.iana.org/assignments/ipsec-registry>.

[isakmp-registry] IANA, "FROM RFC 2407 and RFC 2408 "Magic Numbers" for ISAKMP Protocol", October 2006, <http://www.iana.org/assignments/isakmp-registry>.

[RFC2629] Rose, M.T., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[XML2RFC] Rose, M.T., Fenner, B., and C. Levert, "xml2rfc v1.33", February 2009, <http://xml.resource.org/authoring/README.html>.

[xml2rfc-validator] Fenner, , "xml2rfc validator", January 2007, <http://www.fenron.com/~fenner/ietf/xml2rfc-valid/>.

Адреса авторов

Сергей Е. Леонтьев (editor)
ООО Крипто-Про
Сущёвский вал., д. 16, стр. 5
Москва, 127018
Россия
Phone: +7 (916) 686 10 81
Fax: +7 (495) 780 48 20
EMail: lse@cryptopro.ru
URI: http://www.CryptoPro.ru

Михаил В. Павлов (editor)
ООО Крипто-Про
Сущёвский вал., д. 16, стр. 5
Москва, 127018
Россия
Phone: +7 (495) 780 48 20
Fax: +7 (495) 780 48 20
EMail: pav@cryptopro.ru
URI: http://www.CryptoPro.ru

Андрей А. Федченко (editor)
S-Terra
Зеленоград, МГИЭТ, корпус 10, офис 110
Москва, 124498
Россия
Phone: +7 (495) 726 98 91
Fax: +7 (495) 531 9789
EMail: hell@s-terra.com
URI: http://www.s-terra.ru

A. Совместимость

Требования по реализации алгоритмов:

- AH_GOST-HMAC-4M и GOST-HMAC-4M - обязательно;
- AH_GOST-HMAC-1K и GOST-HMAC-1K - опционально, требуется при повышенных требованиях к безопасности (attacks based on timing and EMI analysis) или для использования IPv6 [JUMBO] пакетов);

Copyright

[TODO: пока секции прав полностью неопределены стоят все возможные Copyright]

Права на интеллектуальную собственность

[TODO: Описать позицию ТК26 относительно прав на интеллектуальную собственность, возможность для российских потребителей использовать результаты ТК26, а так же на потенциальные конфликты интересов]

Всё согласно IETF BCP 78 and BCP 79.