Network Working Group
Request for Comments: 5282
Updates: 4306
Category: Standards Track

D. Black
EMC
D. McGrew
August 2008

Использование алгоритмов аутентифицированного шифрования с элементом Encrypted в протоколе IKEv2

Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol

Статус документа

Этот документ представляет проект стандартного протокола для сообщества Internet и служит приглашением к дискуссии в целях развития и совершенствования протокола. Информацию о текущем состоянии стандартизации протокола можно найти в документе Internet Official Protocol Standards (STD 1). Настоящий документ может распространяться без ограничений.

Аннотация

Алгоритм аутентифицированного шифрования объединяет в одну операцию шифрование и защиту целостности. Такие алгоритмы называют также комбинированными. В этом документе описано использование алгоритмов аутентифицированного шифрования с элементами данных Encrypted протокола IKEv2[1].

Описано также применение двух конкретных алгоритмов аутентифицированного шифрования с элементами IKEv2 Encrypted. Это алгоритм AES[2] в режимах AES GCM[3] и AES CCM[4]. Для использования других алгоритмов аутентифицированного шифрования с элементами IKEv2 Encrypted могут быть разработаны отдельные документы.

Оглавление

[1]Internet Key Exchange version 2 - протокол обмена ключами в Internet версии 2.
[2]Advanced Encryption Standard.
[3]Galois/Counter Mode.
[4]Counter with CBC-MAC Mode.

1. Введение

Алгоритм аутентифицированного шифрования объединяет функции шифрования и защиты целостности в одну операцию над открытым текстом (plaintext) для создания шифрованного текста с контролем целостности [RFC5116]. Для проверки целостности может использоваться значение ICV[1], логически отделённое от зашифрованных данных, или код для проверки целостности может включаться в зашифрованные данные, которые создаются алгоритмом. Алгоритмы аутентифицированного шифрования называют также комбинированным режимом работы блочного шифра (combined mode of operation of a block cipher) или алгоритмами комбинированного режима.

Алгоритм AEAD[2] обеспечивает защиту целостности для дополнительных данных, связанных с открытым текстом и остающихся не зашифрованными. В этом документе описано использование алгоритма AEAD с элементами данных Encrypted в протоколе IKEv2[3]. Описано также использование двух конкретных алгоритмов AEAD с элементами данных IKEv2 Encrypted - AES GCM [GCM] и AES CCM [CCM].

Версия 1 протокола обмена ключами в Internet (IKEv1) [RFC2409] основана на протоколе ISAKMP[4] [RFC2408]. Бит E (Encryption - шифрование) в заголовке ISAKMP говорит о том, что все элементы данных после заголовка зашифрованы, но любая проверка целостности этих элементов обеспечивается отдельным элементом Hash или Signature (см. параграфы 3.1, 3.11 и 3.12 в [RFC2408]). Такое отделение шифрования от защиты целостности препятствует использованию аутентифицированного шифрования в IKEv1, ограничивая использование комбинированного режима AES в IPsec протоколом ESP[5] [RFC2406]. Текущей версией ESP является версия 3 - ESPv3 [RFC4303].

Версия 2 протокола обмена ключами (IKEv2) [RFC4306] использует элементы Encrypted, устроенные на основе ESP. Элемент данных IKEv2 Encrypted связывает шифрование и защиту целостности ток, что становится возможным использование алгоритмов AEAD.

1.1. Используемые соглашения

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].

Символы и переменные для обозначения входных и выходных данных в операциях шифрования и расшифровки (K, N, P, A, C) определены в [RFC5116]. Символы и переменные SK_*, обозначающие конкретные ключи IKEv2, определены в [RFC4306].

2. Структура документа

Этот документ основан на RFC, описывающих использование AES GCM [RFC4106] и AES CCM [RFC4309] с протоколом ESP, поэтому вводный материал и спецификации режимов из этих документов не повторяются здесь. Структура этого документа следует структуре упомянутых и многие параграфы соответствуют параграфам предшественников, а существенные отличия, которые следует принимать во внимание разработчикам, отмечены явно. Существенные части этого документа заимствованы из двух упомянутых RFC.

Этот документ основан на терминологии, обозначениях и интерфейсах аутентифицированного шифрования, описанных в [RFC5116]. Важным отличием от [RFC4106] и [RFC4309] является то, что в этих двух документах процедуры шифрования и защиты целостности разделяются, а [RFC5116] задаёт единый шифрованный выход (ciphertext - C), включающий защиту целостности. Более общий подход включает алгоритмы аутентифицированного шифрования, которые выдают один расширенный шифрованный выход со встроенной защитой целостности вместо раздельного шифрования и защиты целостности.

Для AES GCM и AES CCM шифрованный (C) вывод [RFC5116] аутентифицированного шифрования содержит зашифрованные данные [RFC4106] или [RFC4309], объединённые (конкатенация) со значением кода проверки целостности (ICV[6]) [RFC4106] или [RFC4309]. Этот документ не меняет алгоритмов аутентифицированного шифрования AES GCM и AES CCM, описанных в [RFC4106] и [RFC4309].

3. Элементы данных IKEv2 Encrypted

Этот раздел основан на [RFC5116] и параграфе 3.14 [RFC4306].

Для использования алгоритмов аутентифицированного шифрования с элементами данных IKEv2 Encrypted этот раздел обновляет текст параграфа 3.14 в [RFC4306], меняя рисунок 21 и следующий за ним текст (до конца параграфа) содержимым этого раздела. Кроме того, содержимое параграфа 3.14 в [RFC4306] обновлено также в плане разрешения использовать один алгоритм аутентифицированного шифрования вместо раздельных алгоритмов блочного шифрования и защиты целостности. Параграфы 3.1 и 3.2 этого документа относятся к алгоритмам AES GCM и AES CCM, не меняя, следовательно, документа [RFC4306]. Вносимые этим документом обновления [RFC4306] не оказывают влияния в тех случаях, когда аутентифицированное шифрование не предлагается и не используется.

Структура данных элемента IKEv2 Encrypted применяется для всех алгоритмов аутентифицированного шифрования и эта же структура применяется в ESP. При использовании алгоритма аутентифицированного шифрования элемент IKEv2 Encrypted включает поля заголовка, за которым следует вектор инициализации (IV[7]) и поле шифрованных данных (C[8]), включающее контроль целостности (см. рисунок 1).

Поле Next Payload, флаг C и поле Payload Length не меняются по сравнению с [RFC4306].

[1]Integrity Check Value - значение для проверки целостности.
[2]Authenticated Encryption with Associated Data - аутентифицированное шифрование со связанными данными.
[3]Internet Key Exchange version 2 - протокол обмена ключами в Internet версии 2
[4]Internet Security Association and Key Management Protocol – протокол защищённых связей и обмена ключами.
[5]Encapsulating Security Payload - инкапсулированные защищённые элементы.
[6]Integrity Check Value.
[7]Initialization Vector.
[8]Ciphertext.

Содержимое поля IV определяется алгоритмом аутентифицированного шифрования (см. параграф 3.1 и 4 для алгоритмов AES GCM и AES CCM).

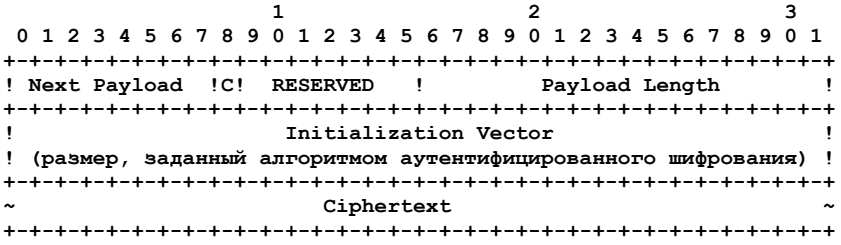

Рисунок 1. Элемент IKEv2 Encrypted с аутентифицированным шифрованием.

Поле Ciphertext представляет собой выход алгоритма аутентифицированного шифрования (см. параграф 2.1 [RFC5116]) для приведённых ниже входных данных.

- Секретный ключ (K) - ключ шифрования, получаемый из ключа SK_ei или SK_er (который подходит), как описано в [RFC4306]. Получение ключа шифрования из SK_ei или SK_er для алгоритмов AES GCM и AES CCM описано ниже в параграфе 7.1.

- Одноразовое значение nonce (N), указываемое алгоритмом аутентифицированного шифрования (для AES GCM и AES CCM см. раздел 4 ниже). При расшифровке элемента Encrypted принимающая сторона создаёт значение nonce на основе вектора инициализации IV в Encrypted с использованием правил для конкретного алгоритма аутентифицированного шифрования (см. параграфы 3.1 и 4 для алгоритмов AES GCM и AES CCM).

- Открытые (нешифрованные) данные (P[1]) представляют собой конкатенацию шифруемых элементов данных IKE с заполнением Padding (если оно используется) и полем Pad Length, как показано ниже на рисунке 2. Структура открытых данных на рисунке 2 применяется для всех алгоритмов шифрования, используемых с элементом IKEv2 Encrypted и не меняется по сравнению с [RFC4306].

- Связанные данные (A[2]), описанные ниже в разделе 5.

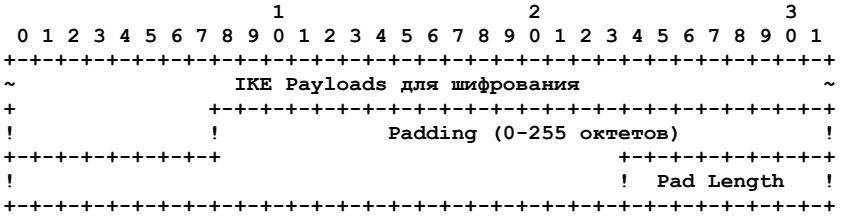

Рисунок 2. IKEv2 Encrypted Payload Plaintext (P).

Элементы данных (поле IKE Payloads) соответствуют [RFC4306].

Поле Padding **может** содержать любое значение, выбранное отправителем.

Поле Pad Length указывает число октетов в поле Padding. К размеру поля Padding не предъявляется требований по выравниванию, получатели **должны** воспринимать заполнение размером от 0 до 255 октетов.

Шифрованный выход алгоритма аутентифицированного шифрования, как определено в [RFC5116], включает в себя данные, которые позволяют проверить целостность и подлинность шифрованной информации и связанных с ней данных. В результате не требуется использовать отдельное поле контроля целостности (ICV[3]) в структуре данных IKEv2 Encrypted.

3.1. Вектор инициализации AES GCM и AES CCM (IV)

Этот параграф основан на параграфах 3.1 из [RFC4106] и 3.1 из [RFC4309]. Требования к векторам инициализации для AES GCM и AES CCM одинаковы и совпадают с требованиями для протокола ESP.

Вектор инициализации (IV) **должен** иметь 8 октетов. Значение IV **должно** выбираться шифрующей стороной (encryptor) так, чтобы то или иное значение IV использовалось только один раз для данного ключа. Шифрующий **может** генерировать IV любым способом, обеспечивающим уникальность значений. Базовые модели генерации IV включают счётчик, инкрементируемый по каждому пакеты и применение линейных регистров сдвига с обратной связью (LFSR[4]).

3.2. Конструкции Ciphertext (C) для AES GCM и AES CCM

Этот параграф основан на разделе 6 из [RFC4106] и параграфе 3.1 из [RFC4309] с обобщением, соответствующим интерфейсам, описанным в [RFC5116]. Конструкции для алгоритмов AES GCM и AES CCM различаются, но в каждом случае они совпадают с конструкциями для ESP.

Для AES GCM и AES CCM поле Ciphertext содержит выход алгоритма аутентифицированного шифрования (отметим, что это поле включает данные контроля целостности).

Значение AES GCM ICV включает только тег аутентификации AES GCM. Реализации **должны** поддерживать полноразмерные 16-октетные значения ICV, **можно** также поддерживать размер 8 или 12 октетов, но **недопустимо** поддерживать другие размеры ICV.

AES CCM использует шифрованное значение ICV. Реализации **должны** поддерживать ICV размером 8 и 16 октетов. **Возможна** также поддержка 12-октетных ICV, но **недопустима** поддержка других размеров ICV.

[1]Plaintext.
[2]Associated data.
[3]Integrity Check Value - код контроля целостности.
[4]Linear feedback shift register - линейный регистр сдвига с обратной связью.

4. Формат Nonce (N) для AES GCM и AES CCM

Конкретные алгоритмы аутентифицированного шифрования **могут** использовать разные форматы одноразовых значений nonce, но им **следует** по умолчанию применять формат nonce, описанный в этом параграфе.

Принятый по умолчанию формат nonce использует частично неявные значения nonce (см. параграф 3.2.1 [RFC5116]) следующим образом:

- неявная часть nonce является «затравкой», которая представляет собой часть ключевого материала IKEv2 (Keying Material), известного шифрующей и дешифрующей стороне (см. параграф 7.1), значение затравки не включается в элемент данных IKEv2 Encrypted;
- явной частью nonce служит вектор инициализации IV, включаемый в элемент IKEv2 Encrypted.

При использовании этого принятого по умолчанию формата nonce шифрующая и дешифрующая сторона создают одноразовое значение nonce путём конкатенации затравки salt с вектором инициализации IV в указанном порядке.

Для использования AES GCM с IKEv2 Encrypted этот принятый по умолчанию формат nonce **должен** использоваться и **должны** применяться 12-октетные значения nonce. Отметим, что этот формат соответствует заданному в разделе 4 [RFC4106], что обеспечивает совместимость между применением AES GCM в IKEv2 и ESP. Все требования раздела 4 [RFC4106] применимы к использованию AES GCM с IKEv2 Encrypted.

Для использования AES CCM с IKEv2 Encrypted этот принятый по умолчанию формат nonce **должен** использоваться и **должны** применяться 11-октетные значения nonce. Отметим, что этот формат соответствует заданному в разделе 4 [RFC4309], что обеспечивает совместимость между применением AES CCM в IKEv2 и ESP. Все требования раздела 4 [RFC4309] применимы к использованию AES CCM с IKEv2 Encrypted.

5. Связанные данные IKEv2 (A)

Этот раздел основан на разделе 5 [RFC4106] и разделе 5 [RFC4309], оба из которых называют связанные данные AAD[1]. Описанная в этом разделе конструкция связанных данных применима для всех алгоритмов аутентифицированного шифрования, но отличается от конструкции, применяемой с ESP, поскольку IKEv2 требует другого покрытия данных в части защиты целостности.

5.1. Конструкция Associated Data (A)

Связанные данные (A) **должны** включать часть содержимого сообщения IKEv2, начиная с первого октета фиксированного заголовка IKE и заканчивая последним октетом Payload Header для элементе Encrypted (т. е., четвёртым октетом элемента Encrypted), как показано на рисунке 3. Это включает все элементы данных между фиксированным заголовком IKE и элементом Encrypted.

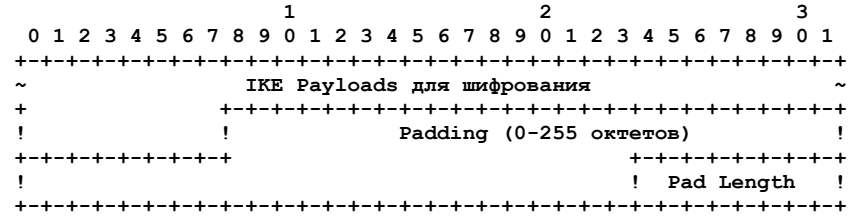

Рисунок 3. Связанные данные (A) элемента IKEv2 Encrypted для аутентифицированного шифрования.

Поля Initialization Vector и Ciphertext, показанные выше на рисунке 1, **недопустимо** включать в связанные данные.

5.2. Охват данных для контроля целостности

Защита целостности IKEv2 Encrypted включает все сообщение IKEv2, содержащее элемент данных Encrypted. При использовании алгоритма аутентифицированного шифрования с элементом Encrypted охват данных реализуется, как показано ниже.

1. Связанные данные (A) охватывают часть сообщения IKEv2, начиная с первого октета фиксированного заголовка IKE и заканчивая последним октетом Payload Header элемента Encrypted (четвёртый октет Encrypted). Сюда включаются все элементы данных между фиксированным заголовком IKE и элементом Encrypted, который всегда является последним элементом данных в сообщении IKEv2 [RFC4306].
2. Вектор инициализации IV служит входными данными для проверки целостности в алгоритме аутентифицированного шифрования. Положительный результат проверки целостности на приёмной стороне подтверждает использование корректного значения IV, обеспечивая защиту целостности и для самого IV.
3. Открытые данные (элементы данных IKE, Padding и Pad Length) охватываются проверкой целостности алгоритма аутентифицированного шифрования.

6. Расширение элементов Encrypted для AES GCM и AES CCM

Расширение, описанное в разделе 7 работы [RFC4106] и разделе 6 работы [RFC4309], применимо к использованию комбинированных режимов AES GCM и AES CCM с элементами данных IKEv2 Encrypted. См. раздел 7 в [RFC4106] и раздел 6 в [RFC4309].

7. Соглашения IKEv2 для AES GCM и AES CCM

В этом разделе описаны соглашения, используемые при генерации ключевого материала и значений «затравок» (salt) для алгоритмов AES GCM и AES CCM с протоколом IKEv2 [RFC4306]. Указаны также идентификаторы и атрибуты, требуемые для использования AES GCM и AES CCM с элементами данных IKEv2 Encrypted.

[1]Additional Authenticated Data - дополнительные аутентифицированные данные.

7.1. Ключевой материал и «затравки»

Этот параграф основан на параграфе 8.1 в [RFC4106] и 7.1 в [RFC4309]. Значения Keying Material и Salt для алгоритмов AES GCM и AES CCM различаются, но имеют структуру, совпадающую со структурой этих полей в ESP.

IKEv2 использует псевдослучайную функцию (PRF[1]) для создания ключевого материала. PRF применяется в режиме итераций для создания ключевого материала произвольного размера, из которого выделяется материал для конкретных целей без учёта выходных границ PRF (см. параграф 2.14 в [RFC4306]).

В этом параграфе показано, как процесс создания ключей, описанный в параграфе 2.14 документа [RFC4306], используется при выработке ключевого материала для AES GCM и AES CCM. Когда алгоритм AES GCM или AES CCM используется с элементами данных IKEv2 Encrypted, ключи защиты целостности SK_ai и SK_ar не применяются и каждый из этих ключей **должен** трактоваться, как значение нулевого размера. Размер ключей шифрования SK_ei и SK_er включает дополнительные байты «затравки» (salt). Размер и формат ключей шифрования SK_ei и SK_er **должен** соответствовать приведённым ниже требованиям.

- Для AES GCM каждый ключ шифрования имеет размер и формат материала «KEYMAT requested», указанного в параграфе 8.1 [RFC4106] для размера ключа AES. Например, если ключ AES имеет размер 128 битов, каждый ключ шифрования будет иметь размер 20 октетов, включающих 16-октетный ключ шифрования AES, за которым следует 4 октета затравки.
- Для AES CCM каждый ключ шифрования имеет размер и формат материала «KEYMAT requested», указанного в параграфе 7.1 [RFC4309] для размера ключа AES. Например, если ключ AES имеет размер 128 битов, каждый ключ шифрования будет иметь размер 19 октетов, включающих 16-октетный ключ шифрования AES, за которым следует 3 октета затравки.

7.2. Идентификаторы преобразований IKEv2

Этот параграф относится только к использованию алгоритмов AES GCM и AES CCM с элементами данных IKEv2 Encrypted. Здесь используются идентификаторы, применяемые для согласования алгоритмов AES GCM и AES CCM в ESP.

Ниже перечислены идентификаторы, выделенные ранее агентством IANA, которые служат для согласования использования в протоколе IKEv2 (т. е., с элементами данных IKEv2 Encrypted) алгоритмов AES GCM и AES CCM в качестве преобразований ENCR:

14 для AES CCM с 8-октетным ICV;

15 для AES CCM с 12-октетным ICV;

16 для AES CCM с 16-октетным ICV;

18 для AES GCM с 8-октетным ICV;

19 для AES GCM с 12-октетным ICV;

20 для AES GCM с 16-октетным ICV.

С IKEv2 **следует** использовать 16-октетные значения ICV, поскольку больший размер ICV обеспечивает более высокий уровень защиты обмена ключами IKEv2 и связанной с этим обменом функциональности.

В общем случае использовать 12-октетные значения (преобразования 15 и 19) **не рекомендуется** с целью снижения числа возможных вариантов размера ICV. Если нужен размер ICV больше 8 октетов, **следует** применять 16-октетные ICV.

7.3. Размер ключа

Этот параграф базируется на параграфе 8.4 в [RFC4106] и параграфе 7.4 в [RFC4309]. Требования к размеру ключа (Key Length) одинаковы для алгоритмов AES GCM и AES CCM и идентичны требованиям для протокола ESP.

Поскольку алгоритм AES поддерживает три размера ключей, атрибут Key Length **должен** указываться при использовании любого из идентификаторов преобразования для AES GCM или AES CCM, перечисленных в параграфе 7.2. Атрибут Key Length **должен** иметь значение 128, 192 или 256. Использовать размер ключа 192 **не рекомендуется**. Если нужен размер ключа AES больше 128 битов, **следует** применять 256-битовый ключ AES. Это снижает число вариантов размера ключа AES.

8. Выбор алгоритма IKEv2

Этот раздел относится к использованию любых алгоритмов аутентифицированного шифрования с элементами IKEv2 Encrypted и не основан на каких-либо предшествующих документах.

IKEv2 (параграф 3.3.3 в [RFC4306]) указывает, что алгоритмы шифрования и защиты целостности требуются для IKE SA[2] (защищённая связь). Этот документ служит обновлением для [RFC4306], указывающим, что при выборе алгоритма аутентифицированного шифрования для любой связи SA (IKE или ESP) **недопустимо** выбирать для этой SA также механизм защиты целостности. Другое обновление [RFC4306] указывает, что в случаях, когда в предложении указаны только алгоритмы аутентифицированного шифрования, в такое предложение **недопустимо** включать какие либо преобразования для защиты целостности.

9. Тестовые векторы

В разделе 9 [RFC4106] и разделе 8 [RFC4309] приведены ссылки, указывающие тестовые векторы для AES GCM и AES CCM.

[1]Pseudo-Random Function.
[2]Security Association.

10. Алгоритмы RFC 5116 AEAD_*

Этот параграф добавляет новые алгоритмы в схему AEAD_*, определённую в [RFC5116], позволяя применять AES GCM и AES CCM с IKEv2. Алгоритмы AEAD_* не имеют каких-либо атрибутов или параметров, идентификатор каждого алгоритма AEAD_*, определённый в данном документе, полностью задаёт размер ключа AES и размер ICV (например, AEAD_AES_128_GCM использует 128-битовый ключ AES и 16-октетное значение ICV).

AEAD_* охватывает алгоритмы аутентифицированного шифрования AES GCM и AES CCM, используемые с IKEv2, и это требует задания 8 дополнительных алгоритмов AEAD_* в дополнение к 4 указанным в [RFC5116]:

- 4 алгоритма AEAD_* задаются для использования 8- и 12-октетных значений ICV с алгоритмом AES GCM и алгоритмами AEAD_*, указанными в [RFC5116].
- Версия AES CCM, применяемая с IPsec (см. [RFC4309]), использует 11-октетные значения nonce вместо 12-октетных в версии AES CCM, указанной в [RFC5116]. 6 алгоритмов AEAD_* указаны для этой версии AES CCM с короткими значениями nonce.

Этот документ рекомендует не применять 192-битовые ключи AES и, следовательно, не включает алгоритмов AEAD_* с такими ключами.

10.1. Алгоритмы AES GCM с 8- и 12-октетными ICV

Следующие 4 алгоритма AEAD_* идентичны алгоритмам AEAD_* из [RFC5116], за исключением использования 8-октетных значений ICV вместо 16-октетных.

10.1.1. AEAD_AES_128_GCM_8

Этот алгоритм идентичен AEAD_AES_128_GCM (параграф 5.1 в [RFC5116]), за исключением тега размера (t) со значением 8 и тега аутентификации размером 8 октетов (64 бита).

Шифротекст AEAD_AES_128_GCM_8 в точности на 8 октетов превышает по размеру нешифрованные данные.

10.1.2. AEAD_AES_256_GCM_8

Этот алгоритм идентичен AEAD_AES_256_GCM (параграф 5.2 в [RFC5116]), за исключением тега размера (t) со значением 8 и тега аутентификации размером 8 октетов (64 бита).

Шифротекст AEAD_AES_256_GCM_8 в точности на 8 октетов превышает по размеру нешифрованные данные.

10.1.3. AEAD_AES_128_GCM_12

Этот алгоритм идентичен AEAD_AES_128_GCM (параграф 5.1 в [RFC5116]), за исключением тега размера (t) со значением 12 и тега аутентификации размером 12 октетов (96[1] битов).

Шифротекст AEAD_AES_128_GCM_12 в точности на 12 октетов превышает по размеру нешифрованные данные.

10.1.4. AEAD_AES_256_GCM_12

Этот алгоритм идентичен AEAD_AES_256_GCM (параграф 5.2 в [RFC5116], за исключением тега размера (t) со значением 12 и тега аутентификации размером 12 октетов (96[2] битов).

Шифротекст AEAD_AES_256_GCM_12 в точности на 12 октетов превышает по размеру нешифрованные данные.

10.2. Алгоритмы AES CCM с 11-октетным Nonce

Следующие 4 алгоритма AEAD реализуют AES CCM с 11-октетным значением nonce, как указано в [RFC4309].

10.2.1. AEAD_AES_128_CCM_SHORT

Алгоритм аутентифицированного шифрования AEAD_AES_128_CCM_SHORT идентичен алгоритму AEAD_AES_128_CCM (см. параграф 5.3 в [RFC5116]), за исключением использования значений nonce на один октет короче. AEAD_AES_128_CCM_SHORT работает в соответствии с [CCM]. Алгоритм использует AES-128 в качестве блочного шифра, обеспечивая для его работы ключ, nonce, связанные данные и открытые данные для шифрования. Форматирование и функция генерации значения счётчика описаны в Приложении A к [CCM], там же указаны значения параметров:

размер nonce - n = 12;

размер тега - t = 16;

q = 3.

Используется тег проверки подлинности размером 16 октетов (128 битов). Шифротекст AEAD_AES_128_CCM_SHORT состоит из шифрованного выхода операции шифрования CCM, объединённого (конкатенация) с выходом тега аутентификации операции шифрования CCM. Тестовые примеры представлены в [CCM]. Размеры входных и выходных данных представлены ниже.

K_LEN - 16 октетов;

P_MAX - 2^{24} - 1 октетов;

A_MAX - 2^{64} - 1 октетов;

N_MIN и N_MAX - по 11 октетов каждое;

[1] В оригинале ошибочно сказано 64. См. https://www.rfc-editor.org/errata_search.php?eid=3605. *Прим. перев.*
[2] В оригинале ошибочно сказано 64. См. https://www.rfc-editor.org/errata_search.php?eid=3606. *Прим. перев.*

C_MAX - 2^{24} + 15 октетов.

Шифротекст AEAD_AES_128_CCM_SHORT в точности на 16 октетов больше соответствующего открытого текста.

10.2.2. AEAD_AES_256_CCM_SHORT

Этот алгоритм идентичен AEAD_AES_128_CCM_SHORT, но имеет пару отличий, показанных ниже:

K_LEN - 32 октета вместо 16;

AES-256 CCM вместо AES-128 CCM.

Шифротекст AEAD_AES_256_CCM_SHORT в точности на 16 октетов больше соответствующего открытого текста.

10.2.3. AEAD_AES_128_CCM_SHORT_8

Этот алгоритм идентичен AEAD_AES_128_CCM_SHORT, отличаясь лишь размером тега проверки подлинности - 8 октетов (64 бита).

Шифротекст AEAD_AES_128_CCM_SHORT_8 в точности на 8 октетов больше соответствующего открытого текста.

10.2.4. AEAD_AES_256_CCM_SHORT_8

Этот алгоритм идентичен AEAD_AES_256_CCM_SHORT, отличаясь лишь размером тега проверки подлинности - 8 октетов (64 бита).

Шифротекст AEAD_AES_256_CCM_SHORT_8 в точности на 8 октетов больше соответствующего открытого текста.

10.2.5. AEAD_AES_128_CCM_SHORT_12

Этот алгоритм идентичен AEAD_AES_128_CCM_SHORT, отличаясь лишь размером тега проверки подлинности - 12 октетов (96[1] битов).

Шифротекст AEAD_AES_128_CCM_SHORT_12 в точности на 12 октетов больше соответствующего открытого текста.

10.2.6. AEAD_AES_256_CCM_SHORT_12

Этот алгоритм идентичен AEAD_AES_256_CCM_SHORT, отличаясь лишь размером тега проверки подлинности - 12 октетов (96[2] битов).

Шифротекст AEAD_AES_256_CCM_SHORT_12 в точности на 12 октетов больше соответствующего открытого текста.

10.3. Алгоритмы AEAD_* и IKEv2

В таблице перечислены алгоритмы AEAD_* AES CCM и AES GCM, которые могут быть согласованы для IKEv2, с указанием идентификаторов преобразования (IKEv2 Encryption (ENCR) Transform Identifier) и размеров ключей (Key Length Attribute), которые применяются при согласовании каждого алгоритма.

Алгоритм AEAD	Идентификатор ENCR	Размер ключа
AEAD_AES_128_GCM	20	128
AEAD_AES_256_GCM	20	256
AEAD_AES_128_GCM_8	18	128
AEAD_AES_256_GCM_8	18	256
AEAD_AES_128_GCM_12	19	128
AEAD_AES_256_GCM_12	19	256
AEAD_AES_128_CCM_SHORT	16	128
AEAD_AES_256_CCM_SHORT	16	256
AEAD_AES_128_CCM_SHORT_8	14	128
AEAD_AES_256_CCM_SHORT_8	14	256
AEAD_AES_128_CCM_SHORT_12	15	128
AEAD_AES_256_CCM_SHORT_12	15	256

Каждый из перечисленных алгоритмов AEAD_* идентичен алгоритму, обозначаемому комбинацией IKEv2 ENCR Identifier и Key Length Attribute, показанной в той же строке таблицы.

11. Вопросы безопасности

Вопросы безопасности, связанные с аутентифицированным шифрованием, рассмотрены в [RFC5116] (см. весь документ, а не только раздел «Вопросы безопасности», поскольку некоторые важные аспекты безопасности рассматриваются за пределами этого раздела).

Вопросы безопасности, связанные с использованием AES GCM и AES CCM с протоколом ESP, применимы и использования этих алгоритмов с IKEv2 Encrypted, как описано в разделе 10 [RFC4106] и разделе 9 [RFC4309]. Применение AES GCM и AES CCM с протоколом IKEv2 не создаёт дополнительных проблем безопасности по сравнению с известными для случая работы AES GCM и AES CCM с протоколом ESP.

Вопросы безопасности IKEv2 рассмотрены в разделе 5 [RFC4306].

12. Взаимодействие с IANA

Идентификаторы преобразований (Encryption Transform), указанные в параграфе 7.2 были выделены IANA для использования с протоколом ESP. Данный документ расширяет их применение на IKEv2 для элементов данных Encrypted. Для такого расширения не требуется каких-либо действий IANA.

[1]В оригинале ошибочно сказано 64 бита. См. https://www.rfc-editor.org/errata_search.php?eid=3605. *Прим. перев.*
[2]В оригинале ошибочно сказано 8 октетов (64 бита). См. https://www.rfc-editor.org/errata_search.php?eid=3606. *Прим. перев.*

Агентство IANA добавило перечисленные в таблице значения в реестр Authenticated Encryption with Associated Data (AEAD) Parameters.

Алгоритм AEAD	Параграф	Идентификатор
AEAD_AES_128_GCM_8	10.1.1	5
AEAD_AES_256_GCM_8	10.1.2	6
AEAD_AES_128_GCM_12	10.1.3	7
AEAD_AES_256_GCM_12	10.1.4	8
AEAD_AES_128_CCM_SHORT	10.1.1	9
AEAD_AES_256_CCM_SHORT	10.1.2	10
AEAD_AES_128_CCM_SHORT_8	10.1.3	11
AEAD_AES_256_CCM_SHORT_8	10.1.4	12
AEAD_AES_128_CCM_SHORT_12	10.1.5	13
AEAD_AES_256_CCM_SHORT_12	10.1.6	14

Регистрация агентством IANA алгоритма AEAD не означает одобрения этого алгоритма или его защищенности.

13. Благодарности

Благодарности за AES GCM и AES CCM приведены в разделе [RFC4106] и разделе 12 [RFC4309].

Благодарим Charlie Kaufman, Pasi Eronen, Tero Kivinen, Steve Kent и Alfred Hoenes за внимательное рецензирование этого документа.

Документ подготовлен с использованием шаблона 2-Word-v2.0.template.dot, автором которого является Joe Touch.

14. Литература

14.1. Нормативные документы

[CCM] Dworkin, M., "NIST Special Publication 800-38C: The CCM Mode for Authentication and Confidentiality", U.S. National Institute of Standards and Technology, <http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf>[1], updated July 2007.

[GCM] Dworkin, M., "NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.", U.S. National Institute of Standards and Technology, November 2007, <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>[2], November 2007.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

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

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

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

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008.

14.2. Дополнительная литература

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

[RFC2408] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

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

Адреса авторов

David L. Black
EMC Corporation
176 South Street
Hopkinton, MA 10748
Phone: +1 (508) 293-7953
EMail: black_david@emc.com

David A. McGrew
Cisco Systems, Inc.
510 McCarthy Blvd.
Milpitas, CA 95035
Phone: +1 (408) 525-8651
EMail: mcgrew@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1]Приведённая ссылка устарела. Документ доступен здесь. *Прим. перев.*
[2]Приведённая ссылка устарела. Документ доступен здесь. *Прим. перев.*