МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т H.235.1

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2005)

СЕРИЯ H: АУДИДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

Инфраструктура аудиовизуальных услуг – Системные аспекты

Безопасность H.323: Базовый профиль защиты

Рекомендация МСЭ-Т H.235.1

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ H

АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

ХАРАКТЕРИСТИКИ ВИДЕОТЕЛЕФОННЫХ СИСТЕМ	H.100–H.199
ИНФРАСТРУКТУРА АУДИОВИЗУАЛЬНЫХ УСЛУГ	
Общие положения	H.200–H.219
Мультиплексирование и синхронизация при передаче	H.220–H.229
Системные аспекты	**H.230–H.239**
Процедуры связи	H.240–H.259
Кодирование движущихся видеоизображений	H.260–H.279
Сопутствующие системные аспекты	H.280–H.299
Системы и оконечное оборудование для аудиовизуальных услуг	H.300–H.349
Архитектура услуг справочника для аудиовизуальных и мультимедийных услуг	H.350–H.359
Качество архитектуры обслуживания для аудиовизуальных и мультимедийных услуг	H.360–H.369
Дополнительные услуги для мультимедиа	H.450–H.499
ПРОЦЕДУРЫ МОБИЛЬНОСТИ И СОВМЕСТНОЙ РАБОТЫ	
Обзор мобильности и совместной работы, определений, протоколов и процедур	H.500–H.509
Мобильность для мультимедийных систем и услуг серии H	H.510–H.519
Приложения и услуги мобильной мультимедийной совместной работы	H.520–H.529
Защита мобильных мультимедийных систем и услуг	H.530–H.539
Защита приложений и услуг мобильной мультимедийной совместной работы	H.540–H.549
Процедуры мобильного взаимодействия	H.550–H.559
Процедуры взаимодействия мобильной мультимедийной совместной работы	H.560–H.569
ШИРОКОПОЛОСНЫЕ И МУЛЬТИМЕДИЙНЫЕ TRIPLE-PLAY УСЛУГИ	
Предоставление широкополосных мультимедийных услуг по VDSL	H.610–H.619

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т H.235.1

Безопасность H.323: Базовый профиль защиты

Резюме

В данной Рекомендации рассмотрена аутентификация и защита целостности, или "только аутентификация" для RAS H.225.0 и сигнализации вызова, H.225.0, и туннелированных H.245, использующих основанную на пароле защиту RAS H.225.0 с хэшированием HMAC-SHA1-96 и сообщений Сигнализации вызова посредством использования защитных методов криптографии, основанных на паролях. Профиль защиты применим к вариантам: оконечное устройство H.323 – привратник, привратник-привратник, шлюз H.323 – привратник и других объектов H.323 в администрируемых средах с присвоенными симметричными ключами/паролями.

В более ранних версиях подсерии H.235, этот профиль содержался в Приложении D/H.235. В Дополнениях IV, V, VI к H.235.0 показано полное соответствие пунктов, рисунков, и таблиц между версиями 3 и 4 H.235.

Источник

Рекомендация МСЭ-Т H.235.1, утвержденная 13 сентября 2005 г. МСЭ-Т 16-й Исследовательской комиссией (2005–2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

Ключевые слова

Аутентификация, сертификат, цифровая подпись, шифрование, целостность, управление ключом, защита мультимедиа, профиль защиты.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т H.235.1

Безопасность H.323: Базовый профиль защиты

1 Сфера применения

В данной Рекомендации рассмотрена аутентификация и защита целостности, или "только аутентификация" для RAS H.225.0 и сигнализации вызова, H.225.0, и туннелированных сообщений H.245, использующих основанную на пароле защиту RAS H.225.0 с хэшированием HMAC-SHA1-96 и сообщений Сигнализации вызова посредством использования защитных методов криптографии, основанных на паролях. Профиль защиты применим к вариантам: оконечное устройство H.323–привратник, привратник–привратник, шлюз H.323–привратник и других объектов H.323.

2 Справочные документы

2.1 Нормативные справочные документы

В перечисленных ниже Рекомендациях МСЭ-Т и другой справочной литературе содержатся положения, которые посредством ссылок на них в этом тексте составляют основные положения данной Рекомендации. На момент опубликования действовали указанные редакции документов. Все Рекомендации и другая справочная литература являются предметом корректировки, и стороны пришли к договоренности основываться на этой Рекомендации и стараться изыскивать возможность для использования самых последних изданий Рекомендации и справочной литературы перечисленной ниже. Регулярно публикуется перечень действующих Рекомендаций МСЭ-Т. Ссылка на документ в рамках этой Рекомендации не дает ему, как отдельному документу, статуса Рекомендации.

– Рекомендация МСЭ-Т H.225.0 (2003 г.), *Протоколы сигнализации о соединении и пакетирование потоков носителей для мультимедийных систем связи на основе пакетов.*

– ITU-T Recommendation H.235 version 1 (1998), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*.

– ITU-T Recommendation H.235 version 2 (2000), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*.

– ITU-T Recommendation H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.

– ITU-T Recommendation H.235.2 (2005), *H.323 security: Signature security profile*.

– ITU-T Recommendation H.235.4 (2005), *H.323 security: Direct and selective routed call security*.

– ITU-T Recommendation H.235.6 (2005), *H.323 security: Voice encryption profile with native H.235/H.245 key management*.

– Рекомендация МСЭ-Т H.245 версия 10 (2003 г.), *Управляющий протокол для мультимедийной связи.*

– Рекомендация МСЭ-Т H.323 (2003 г.), *Мультимедийные системы связи на основе пакетов*.

– ITU-T Recommendation H.323 Annex F (1999), *Simple endpoint types*.

– ITU-T Recommendation Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control*.

– ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

ISO/IEC 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

– ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

– ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

– ITU-T Recommendation X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

– ISO/IEC 10118-3:2004, *Information Technology – Security techniques – Hash-functions* – Part 3: *Dedicated hash-functions*.

2.2 Информативные справочные документы

[FIPSPUB180-2] Federal Information Processing Standard FIPS PUB 180-2, Secure Hash Standard, U. S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 1 August 2002.

[OIW] Stable Implementation – Agreements for Open Systems Interconnection Protocols: Part 12 – OS Security; Output from the December 1994 Open Systems Environment Implementors' Workshop (OIW); http://nemo.ncsl.nist.gov/oiw/agreements/stable/OSI/12s_9412.txt.

[RFC2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.

[WEBOIDs] http://www.alvestrand.no/objectid/top.html.

3 Термины и определения

Согласно целям настоящей Рекомендации, определения, данные в пунктах 3/H.323, 3/H.225.0 и 3/H.245 применяются вместе с данными в этом пункте. Некоторые из терминов, используемых в этой Рекомендации, также определены в Рекомендациях МСЭ-Т X.800 | ISO 7498-2, X.803 | ИСО/МЭК 10745, X.810 | ИСО/МЭК 10181-1 и X.811 | ИСО/МЭК 10181-2.

В этой Рекомендации используются следующие термины для обеспечения услуг защиты.

3.1 аутентификация и целостность: Это смешанная часть услуг защиты базового профиля, которая поддерживает целостность сообщений в сочетании с аутентификацией пользователя. Пользователь может обеспечить аутентификацию правильным применением процедуры общего секретного ключа. Обе услуги защиты обеспечиваются одним и тем же механизмом защиты.

3.2 "**только аутентификация**": Эта услуга защиты, предлагаемая в базовом профиле защиты, как альтернатива, поддерживает аутентификацию только выбранных полей, но не обеспечивает полной целостности сообщений. Профиль защиты с "только аутентификацией" применим для сообщений сигнализации, проходящих через устройства NAT/сетевых экранов. Пользователь может обеспечить аутентификацию правильным применением процедуры общего секретного ключа.

При использовании методов симметричного шифрования, услуги защиты аутентификация/целостность применимы только на переходной основе.

4 Символы и сокращения

В данной Рекомендации используются следующие символы и сокращения:

ASN.1 Абстрактная синтаксическая нотация версии 1

EP Конечная точка

EPID Идентификатор конечной точки

GK	Привратник
GKID	Идентификатор привратника
GRQ	Запрос привратника
HMAC	Хэшированный код аутентификации сообщения
ICV	Значение проверки целостности
ITU	Международный союз электросвязи
LRQ	Запрос местонахождения
MAC	Код аутентификации сообщения
NAT	Трансляция сетевого адреса
OID	Идентификатор объекта
RAS	Регистрация, допуск и статус
RTP	Протокол режима реального времени
SHA	Алгоритм защитного хэширования
TCP	Протокол контроля передачи
UTC	Идущие по всемирному времени часы
VoIP	Голосовая связь по протоколу Интернет

5 Соглашения по терминам

В данной Рекомендации используются следующие соглашения:

– "должен" означает обязательное требование.

– "следует" означает предлагаемый, но не обязательный ход действий.

– "может" означает скорее необязательный ход действий, чем рекомендацию о том, что что-либо должно иметь место.

В данной Рекомендации определяется **базовый профиль защиты**. Базовый профиль защиты обеспечивает основную защиту простыми средствами, используя защитные методы криптографии, основанные на паролях. Этот базовый профиль защиты может быть использован совместно с такими профилями защиты, как H.235.3, H.235.4, H.235.5, H.235.6 и H.235.7.

В данной Рекомендации используются поля H.235 для обеспечения услуг защиты аутентификации/целостности в сообщениях сигнализации H.323. Различные идентификаторы объектов (см. пункт 15) определяют, какое устройство защиты фактически выбрано и какая версия протокола данной Рекомендации используется. В Процедуре I изложено, как использовать услуги защиты в определенных механизмах защиты, таких как симметричные (хэширование с ключом) методы. Идентификаторы объектов приведены в качестве ссылок в виде символических обозначений в тексте (например "A"), см. также пункт 5/H.235.0.

Несмотря на то, что услуга обеспечения целостности всегда обеспечивает также и аутентификацию сообщений, обратное не всегда верно. На практике, совместная услуга обеспечения целостности и аутентификации использует один и тот же материал ключа, без внедрения слабостей защиты.

Более того, вся переходная информация защиты помещается в элемент **CryptoHashedToken**. Эта информация вычисляется заново на каждом переходе.

В данной Рекомендации применяются определенные методы симметричного шифрования в целях аутентификации и обеспечения целостности. В этом тексте используются термины пароль и общий секрет, когда применяются симметричные методы.

В общем, пароль, сеансовый ключ и общий секрет имеют общим то, что все они используются в симметричном шифровании между двумя (или более) объектами. Разница между паролем и сеансовым ключом/общим секретом заключается в том, как в действительности применяются ключи, например, пароли – для аутентификации и авторизации, сеансовые ключи – для шифрования. Термин "общий секрет" как бы нейтрален и в действительности не относится к какому-либо специфическому использованию.

Пароль (может рассматриваться также как общий секрет) используется для аутентификации/обеспечения целостности RAS и H.225.0, так как этот элемент может вводиться пользователем. Пароль обычно представляет собой буквенно-цифровую строку, которую пользователи могут запомнить. Пароль обычно имеет длительное время жизни; пароль известен *априорно* и может быть определен как часть всего процесса подписания пользователем. Какой-нибудь алгоритм (например, пропускание пароля через алгоритм хэширования) может преобразовать пароль для более удобной обработки в протоколах для того, чтобы получить фиксированную длину.

Очевидно, что использование паролей должно происходить с особой осторожностью. Пароли могут обеспечить достаточную защиту, только когда они выбираются случайно из большого пространства, когда они несут достаточную энтропию, такую, что они непредсказуемы, и когда они их периодически меняют. Правила, касающиеся установления и хранения паролей, лежат вне области применения данной Рекомендации.

Хорошей практикой получения выгоды от использования паролей и общего секрета может являться преобразование строки пароля пользователя в фиксированную битовую строку общего секрета с использованием криптографически сильной односторонней хэш-функции.

В качестве рекомендуемого примера, при использовании профиля защиты данной Рекомендации, SHA1 при применении к строке пароля дает 20-байтовый общий секрет. Преимущество состоит в том, что хэшированный результат не только скрывает настоящий пароль, но и определяет формат битовой строки фиксированной длины, не жертвуя для этого энтропией.

Таким образом,

общий секрет:= SHA1 (пароль).

В **ClearToken** H.235 предлагается поле, называемое **random**, содержащее 32-битное целое число. Это поле используется в следующем смысле: **random** фактически представляет собой монотонно возрастающее число, начинающееся с какого-либо значения и возрастающее с каждым выходящим сообщением. Поле **random** используется в качестве дополнительного "рандомизирующего" значения для ввода в хэш-функцию с ключом в случае, когда несколько сообщений быстро посылаются одно за другим, тем не менее передавая одинаковые временные отметки. Такое может происходить, когда часы UTC не обеспечивают достаточного разрешения часов. По существу, произведенное значение хэша или значение проверки целостности выглядят различными из-за изменяющегося значения **random**. Это препятствует атакам взлома защиты путём замещения оригинала (атакам воспроизведения). Для упрощения использования здесь более предпочтителен возрастающий счетчик, чем по-настоящему случайная последовательность. Получатель может хранить полученные пары **timestamp**/**random** в течение периода, определяемого окном местного времени. Атаки воспроизведения можно выявить, когда одна и та же пара **timestamp/random** встречается дважды.

ПРИМЕЧАНИЕ. – Окно времени компенсирует изменения синхронизации времени и задержку переходов сети.

В этом профиле определяется "установление **generalID** в **ClearToken** на идентификатор получателя". В действительности это означает, что для сообщений RAS, предназначенных привратнику, это идентификатор привратника; для сообщений RAS, предназначенных конечной точке, это идентификатор конечной точки; для сообщений сигнализации вызова H.225.0, предназначенных привратнику, это идентификатор привратника и для сообщений сигнализации вызова H.225.0, предназначенных конечной точке, это идентификатор названной конечной точки, см. также пункт 14.

sendersID должен быть установлен на строку идентификации отправителя. В действительности это означает, что для сообщений RAS, предназначенных привратнику, это идентификатор конечной точки; для сообщений RAS, предназначенных конечной точке, это идентификатор привратника; для сообщений сигнализации вызова H.225.0 предназначенных привратнику, это идентификатор привратника и для всех сообщений сигнализации вызова H.225.0, предназначенных конечной точке, это идентификатор названной конечной точки, см. также пункт 14.

В данной Рекомендации может применяться защита целостности сообщений, которая охватывает все сообщение. Для RAS H.225.0, защита целостности покрывает все целиком сообщение RAS; для сигнализации вызова, она покрывает целиком все сообщение сигнализации вызова H.225.0, включая заголовки Q.931.

В данной Рекомендации используются хорошо известные термины защиты, такие как ключ, управление ключом и SET, которые имеют отличные значения в других контекстах (например, панель с сенсорными кнопками, управление клавишами Q.931/Q.932, и протокол электронных транзакций защиты).

6 Обзор

В данной Рекомендации рассмотрена аутентификация и защита целостности, или "только аутентификация" для RAS H.225.0 и сигнализации вызова, H.225.0, и туннелированных сообщений H.245, использующих основанную на пароле защиту RAS H.225.0 с хэшированием HMAC-SHA1-96 и сообщений сигнализации вызова посредством использования защитных методов криптографии, основанных на паролях. Профиль защиты применим к вариантам: оконечное устройство H.323-привратник, привратник-привратник, шлюз H.323-привратник и других объектов H.323 в администрируемых средах с присвоенными симметричными ключами/паролями.

6.1 Кратко о характеристиках обеспечения защиты

Возможности, предусмотренные этими профилями, включают:

– для RAS, H.225.0 и туннелированных сообщений H.245:

  - Аутентификация пользователя желаемому объекту, независимая от числа переходов прикладного уровня, через которые проходит сообщение.

    ПРИМЕЧАНИЕ. – Переход понимается здесь в значении доверенного сетевого элемента H.235 (например, привратник, шлюз, MCU, прокси, сетевой экран). Таким образом, переходная защита прикладного уровня при использовании с симметричными методами не обеспечивает достоверной сквозной защиты между оконечными устройствами.

  - Сама по себе целостность сообщения сигнализации, включающая критические порции (поля) сообщений, прибывающих на объект, независимая от числа переходов прикладного уровня, через которые проходит сообщение.
  - Переходная аутентификация и целостность сообщений сигнализации прикладного уровня обеспечивают эти услуги защиты для всего сообщения.

Обеспечением вышеописанных услуг защиты подходящим образом можно помешать исполнению нескольких атак. Они включают:

- Атаки типа "отказ от обслуживания": Такие атаки может предотвратить быстрая проверка значений криптографического хэша.
- Атаки через посредника: Переходная аутентификация и целостность сообщений прикладного уровня предотвращает такие атаки, когда посредник находится между переходами прикладного уровня, скажем, враждебный маршрутизатор.
- Атаки замещения оригинала (атаки воспроизведения): Такие атаки предотвращает использование временных отметок и чисел последовательности.
- Имитация соединения: Такие атаки предотвращает аутентификация пользователя.
- Захват соединения: Такие атаки предотвращает аутентификация/целостность каждого сообщения сигнализации.

Другие важные черты простого профиля защиты включают:

- Использование надежных, хорошо известных и широко применяемых алгоритмов на основе материала IMTC/ETSI/IETF.
- Возможность использования в местах действия на основе требований защиты бизнес-модели.
- Применимость к различным сценариям использования, таким, как в закрытых группах, и для масштабируемых сред и в многоточечных конференциях.

- Профиль защиты с "только аутентификацией" применим, когда предусмотрены какие-нибудь средства защиты для прохода через NAT/сетевой экран.

В таблице 1 подводится итог по всем процедурам профилей защиты, имеющих дело с различными требованиями защиты, определенным в данной Рекомендации. Дополнительный профиль защиты "только аутентификации" показан диагональной штриховкой – голубым в электронной копии.

Таблица 1/H.235.1 – Базовый профиль защиты

Услуги защиты	**Функции вызова**			
	RAS	**H.225.0**	**H.245 (Примечание)**	**RTP**
Аутентификация	Пароль HMAC-SHA1-96	Пароль HMAC-SHA1-96	Пароль HMAC-SHA1-96	
"Только аутентификация"	Пароль HMAC-SHA1-96	Пароль HMAC-SHA1-96	Пароль HMAC-SHA1-96	
Неотказуемость				
Целостность	Пароль HMAC-SHA1-96	Пароль HMAC-SHA1-96	Пароль HMAC-SHA1-96	
Конфиденциальность				
Контроль доступа				
Управление ключом	Присвоение пароля на основе подписи			
ПРИМЕЧАНИЕ. – Туннелированные H.245 или встраиваемые H.245 внутрь быстрого соединения H.225.0				

Для аутентификации пользователь должен использовать схему не основе пароля. Схема на основе пароля крайне рекомендуется для аутентификации вследствие своей простоты и легкости применения. Для достижения целостности сообщений рекомендуется хэширование всех полей в RAS H.225.0 и сообщениях сигнализации вызова (также используя схему с паролем).

В защищенных объектах H.323 с этим профилем защиты осуществляется аутентификация совместно с целостностью при использовании одного и того же общего механизма защиты.

Методы контроля доступа подробно не изложены; их можно использовать локально с помощью полученной информации, содержащейся в полях сигнализации H.235 (ClearToken, CryptoToken).

В этой рекомендации не описываются процедуры назначения пароля/секретного ключа на основе подписей с менеджментом и администрированием. Такие процедуры можно осуществить средствами, выходящими за рамки обзора данной Рекомендации.

Объекты, вовлеченные в процесс передачи информации способны неявно определить использование либо базового, либо с подписями профиля защиты путем оценки сигнализированных идентификаторов объектов защиты в сообщениях (**tokenOID**, и **algorithmOID**; см. также пункт 15).

6.2 Применимость базового профиля защиты

Базовый профиль защиты применим в среде, где подписанные пароли/симметричные ключи могут быть присвоены защищенным объектам H.323 (оконечным устройствам) и сетевым элементам (привратник, прокси). Он обеспечивает аутентификацию и целостность, или "только аутентификацию" для RAS H.225.0 и сигнализации вызова, H.225.0 и туннелированных H.245, используя основанный на пароле хэш HMAC-SHA1-96, как изложено в процедуре I. H.225.0, установления соединения, используя FastStart (привратник-привратник или оконечное устройство-оконечное устройство), включает интегрированное управление ключом со схемой Диффи-Хеллмана.

В базовом профиле защиты предписывается использование процедуры быстрого установления соединения и рекомендуется использовать туннелирование H.245 внутри H.225.0

6.3 Требования H.323

Объекты H.323, использующие этот профиль защиты предполагают поддержку следующих возможностей H.323:

- быстрое соединение;
- модель с маршрутизированным привратником.

6.4 Обзор процедур

Для использования в этом профиле описана следующая процедура.

Процедура I представляет собой простой механизм аутентификации сообщений сигнализации на основе симметричного ключа, основанный на общем пароле между двумя объектами (например, привратник и конечная точка H.323). Эта процедура обеспечивает аутентификацию и целостность сообщений RAS, Q.931 и H.245 (см. пункт 7).

Процедура IA представляет собой простой механизм "только аутентификации" сообщений сигнализации на основе симметричного ключа, основанный на общем пароле между двумя объектами (например, привратник и конечная точка H.323). Эта процедура обеспечивает "только аутентификацию", но не обеспечивает целостность всего сообщения. Альтернатива с "только аутентификацией" применима в сценариях, где сообщения сигнализации H.323 проходят через NAT/сетевые экраны.

В зависимости от политики защиты, аутентификации может быть односторонней или двусторонней с применением аутентификации/целостности в обратном направлении, таким образом, заодно и обеспечивая более высокую безопасность. Привратник решает, применять ли аутентификацию/целостность еще и в обратном направлении.

Привратники, обнаруживающие неудавшуюся аутентификацию и/или неудавшуюся проверку целостности в сообщении RAS или сообщении Сигнализации вызова, полученном от защищенной конечной точки или равного привратника, отвечают соответствующим сообщением отказа, отражающим сбой защиты путем установки причины отказа в **securityDenial**, или другой подходящий код ошибки защиты, согласно 11.1/H.235.0. В зависимости от возможности распознать атаку и наиболее подходящего способа реакции на нее, привратник, получающий защищенный **xRQ** с неопределенными идентификаторами объектов (**tokenOID**, **algorithmOID**), может ответить незащищенным **xRJ** и отказаться с указанием причины, установленным в **securityDenial**, или может отклонить это сообщение. Встреченное событие защиты следует записать в журнал. С другой стороны, конечная точка должна отклонить полученное незащищенное сообщение, выждать и может попытаться вновь, рассматривая выбор других OID. Подобным образом, привратник, получающий защищенное сообщение SETUP H.225.0 с неопределенными идентификаторами объектов (**tokenOID**, **algorithmOID**) может ответить незащищенным RELEASE COMPLETE и причиной отказа, установленной в **securityDenied**, или может отклонить сообщение. Подобным образом, встреченное событие защиты следует записать в журнал.

Существует скрытая сигнализация H.235 для показания использования процедуры I и применяемого механизма защиты, основанная на значениях идентификаторов объектов (см. также пункт 15) и заполненных полях сообщения.

В профиле не используются поля ICV H.235; лучше рассматривать значения проверки целостности шифрования как значения криптографического хэша и помещать в поля хэша **CryptoToken**.

7 Аутентификация и целостность сообщений сигнализации на основе симметричного ключа (процедура I)

Когда выполняется процедура I, нужно следовать нижеописанным процедурам:

- В алгоритме HMAC-SHA1-96 генерируется 12-байтовое (96-битное) значение хэша в качестве результирующего аутентификатора. Если ключ генерируется из пароля, то для вычисления ключа из пароля *должен* использоваться механизм, описанный в 8.2.4/H.235.0.

  ПРИМЕЧАНИЕ 1. – Когда секретный ключ получают из введенного пользователем пароля, следует отнестись с должным вниманием, чтобы гарантировать достаточную случайность. Рекомендуется, например, использовать действительно случайные секреты для секретного ключа, или убедиться, что случайные пароли достаточно длинные.

- Поле **CryptoH323Token** в каждом сообщении RAS/H.225.0 должно содержать следующие поля:

– **nestedCryptoToken**, содержащее **CryptoToken**, которое само содержит **cryptoHashedToken**, содержащее следующие поля:

• **tokenOID**, установленное в "A", это показывает, что вычисление аутентификации/целостности включает все поля в RAS H.225.0 и сообщении сигнализации вызова.

• **hashedVals**, содержащее поле **ClearToken**, используемое со следующими полями:

– **tokenOID** установлено в "T", это показывает, что базовый **ClearToken**, как показано выше используется для аутентификации сообщений и защиты от атак воспроизведения, а также для управления ключом Диффи-Хеллмана, как описано в 8.5/H.235.6. В качестве альтернативы, вместо базового ClearToken, могут быть использованы другие ClearToken с другими OID.

– **timeStamp** содержит временную отметку.

– **random** содержит число монотонно возрастающей последовательности. Это число допускает конструкции из двух сообщений с одной временной отметкой (в пределах разрешения часов).

– **generalID** содержит идентификатор получателя (только в случае одноадресных сообщений).

– **sendersID** содержит идентификатор отправителя.

– **dhkey**, используется для прохода параметров Диффи-Хеллмана, как изложено в этой Рекомендации во время **Setup** на **Connect**.

• **halfkey** содержит случайный открытый ключ одной группы.

• **modsize** содержит основную часть простого числа DH (Диффи-Хеллмана) (см. таблицу 4/H.235.6).

• **generator** содержит группу DH (см. таблицу 4/H.235.6).

ПРИМЕЧАНИЕ 2. – Когда базовый профиль безопасности используется без защитного профиля голосового шифрования, то никакие параметры Диффи-Хеллмана не должны посылаться и **dhkey** должен отсутствовать; **halfkey**, **modsize** и **generator** могут быть установлены в {'0'B,'0'B,'0'B}.

– **token**, содержащее **HASHED** с полями:

• **algorithmOID**, установленным в "U", что показывает использование HMAC-SHA1-96.

• **params**, установленным в NULL.

• **hash** содержащим аутентификатор, вычисленный с использованием HMAC-SHA1-96. Этот аутентификатор может быть вычислен по:

– всем полям RAS H.225.0 и сигнализации вызова сообщения, если **tokenOID** в **CryptoHashedToken** установлено в "A" (что показывает аутентификацию и целостность).

tokenOID "A" используется для защиты туннелированных H323-UU-PDU, включая всё содержимое сообщений H.245; вычисление хэша должно быть произведено над всем сообщением сигнализации вызова **H.225.0** со всеми полями, согласно процедуре, описанной в 7.3.

• Аутентификатор проверяется в конце каждого завершающего канал отрезка (как варианты возможны конечная точка 1-привратник 1, конечная точка 1-привратник 2, привратник 2-конечная точка 2, конечная точка 1-привратник 2, привратник 1-конечная точка 2 или конечная точка 1-конечная точка 2), и повторно рассчитывается перед отправкой сообщения на следующий отрезок.

ПРИМЕЧАНИЕ 3. – Аутентификатор вычисляется на основе каждого отдельного сообщения.

ПРИМЕЧАНИЕ 4. – Должен использоваться метод дополнения битами внутри стандарта SHA1 (ИСО/МЭК 10118-3).

ПРИМЕЧАНИЕ 5. – Когда совместно используются аутентификация и целостность, аутентификатор вычисляется по всему сообщению.

ПРИМЕЧАНИЕ 6. – Для того чтобы предупредить возможность атак воспроизведения, строго рекомендуется гарантировать в реализациях, чтобы пароль (ключ) менялся перед изменением (или завершением цикла) числа монотонно возрастающей последовательности.

ПРИМЕЧАНИЕ 7. – Получатель способен обнаружить использование процедуры I путем оценки **tokenOID** внутри хэшированного **EncodedGeneralToken** (обнаружение присутствия "A").

7.1 Вычисление хэша на основе пароля

И отправитель, и получатель аутентифицированного/с защищенной целостностью сообщения вычисляют хэш с ключом по всем полям кодированного ASN.1 сообщения (с использованием OID "A"). Что касается профиля с "только аутентификацией", и отправитель, и получатель вычисляют зашифрованный хэш по всем кодированным ASN.1 ClearToken (с использованием OID "B").

7.2 HMAC-SHA1-96

HMAC-SHA1-96 представляет собой усеченное 96-битное значение криптографического хэша 160-битного вычисления SHA1. В качестве результата должны использоваться 96 крайних битов представления сетевого байтового порядка значения хэша. В RFC 2104 описывается процедура с секретным ключом *K* установленным на общий секрет (= хэшированный SHA1 пароль) и *text,* установленным на буфер сообщения.

7.3 Вычисление и проверка аутентификации и целостности

Для аутентификации и целостности сообщения (в случае, когда применяется OID "A") существует следующая процедура.

Отправитель сообщения должен вычислять хэш как следует ниже:

1) Установить значение хэша в специфический шаблон "по умолчанию" длиной 96 битов. Выбор точного битового шаблона не имеет значения, но хорошим выбором является уникальный битовый шаблон, который не встречается в остальной части сообщения.
2) ASN.1 – зашифровать все сообщение; для RAS оно включает все сообщение RAS H.225.0; для сигнализации вызова оно включает все сообщение сигнализации вызова H.225.0.
3) Обнаружить шаблон "по умолчанию" в зашифрованном сообщении; переписать весь найденный битовый шаблон 96 нулевыми битами.

   ПРИМЕЧАНИЕ 1. – Обнаружение может повлечь некоторые шаги метода проб и ошибок в редких случаях, когда шаблон "по умолчанию" встречается в сообщении более чем единожды.
4) Вычислить значение криптографического хэша по шифрованному ASN.1 сообщению с использованием HMAC-SHA1-96 (см. 7.2).
5) Заменить шаблон "по умолчанию" в шифрованном сообщении вычисленным значением хэша.

Получатель принимает сообщение и затем действует следующим образом:

1) ASN.1 – дешифрует сообщение.
2) Извлекает полученное значение хэша и сохраняет его в локальной переменной RV.
3) Ищет и обнаруживает значение хэша RV в полученном шифрованном сообщении.

   ПРИМЕЧАНИЕ 2. – В редких случаях, где подстрока значения хэша во всем сообщении может встретиться несколько раз, шаги 3–6 должны быть последовательно повторены с другой начальной позиции поиска.
4) Переписывает весь битовый шаблон в шифрованном сообщении 96 нулями.
5) Вычисляет значение криптографического хэша по шифрованному сообщению с использованием HMAC-SHA1-96 (см. пункт 7.2).
6) Сравнивает RV с вычисленным значением хэша. Сообщение считается неиспорченным, только если оба значения хэша равны; В этом случае аутентификация прошла успешно и процедура останавливается.
7) В противном случае, повторяет шаги 3–7, восстанавливая RV в предыдущее положение, и ищет другие совпадения. Если ни одно из совпадений не дает корректного сравнения значений хэша, то аутентификация не удалась, и сообщение было изменено (случайно или намеренно) во время передачи.

8 "Только аутентификация" (процедура IA)

В оконечных устройствах может быть выбрано использование "только аутентификации" (используя OID "B", см. пункт 20/H.235.2). В этом случае, аутентификатор вычисляется только по подряду (**ClearToken** внутри **CryptoToken**) сообщения RAS/H.225.0. "Только аутентификация" может быть полезной для прохождения через NAT/сетевые экраны, которые меняют IP адреса/порты внутри полезных данных H.323.

Так как аутентификация охватывает только очень малую долю сообщения, "только аутентификация" не обеспечивает целостности сообщения, какую предоставляет процедура I. Соответственно, "только аутентификация" обеспечивает меньшую защиту.

Для "только аутентификации", в защищенных сообщениях должны быть использованы следующие поля:

- Поле **CryptoH323Token** в каждом сообщении RAS/H.225.0 должно содержать следующие поля:
  - **nestedCryptoToken** содержащее **CryptoToken**, которое само по себе содержит **cryptoHashedToken**, содержащее следующие поля:
    - **tokenOID** установленное в:
      - "B" (см. пункт 20/H.235.2), это показывает, что вычисление "только аутентификации" включает все поля в **ClearToken**.
    - **hashedVals** содержащее поле **ClearToken** используемое со следующими полями:
      - **tokenOID** установлено в:
        - "T" (как пример базы ClearToken для оставшегося содержимого ClearToken) или какой-либо другой OID для каких-либо других целей.
      - **timestamp** содержит временную отметку;
      - **random** содержит число монотонно возрастающей последовательности. Это число позволяет сделать два сообщения с одной и той же временной отметкой (в пределах разрешения часов) уникальными;
      - **generalID** содержит идентификатор получателя (только в случае одноадресных сообщений);
      - **sendersID** содержит идентификатор отправителя;
      - **dhkey**, используется для прохода параметров Диффи-Хеллмана как изложено в Рек. МСЭ-Т H.235.0 во время **Setup** на **Connect**.
        - **halfkey** содержит случайный открытый ключ одной группы;
        - **modsize** содержит основную часть простого числа DH (Диффи-Хеллмана) (см. таблицу 4/H.235.6);
        - **generator** содержит группу DH (см. таблицу 4/H.235.6).

        ПРИМЕЧАНИЕ 1. – Когда базовый профиль защиты используется без защитного профиля голосового шифрования, то никакие параметры Диффи-Хеллмана не должны посылаться и **dhkey** должен отсутствовать; **halfkey**, **modsize** и **generator** могут быть установлены в {'0'B,'0'B,'0'B}.
  - **token** содержащее **HASHED** с полями:
    - **algorithmOID** установленным в "U", что показывает использование HMAC-SHA1-96;
    - **params** установленным в NULL;
    - **hash** содержащим аутентификатор, вычисленный с использованием HMAC-SHA1-96. Аутентификатор должен быть вычислен по:
      - всем полям в **ClearToken**, если **tokenOID** в **CryptoHashedToken** установлено в "B" (что показывает "только аутентификацию").
- Аутентификатор проверяется в конце каждого завершающего канал отрезка (как варианты, возможны конечная точка 1-привратник 1, привратник 1-привратник 2, привратник 2-конечная точка 2, конечная точка 1-привратник 2, привратник 1-конечная точка 2 или конечная точка 1-конечная точка 2), и повторно рассчитывается перед отправкой сообщения на следующий отрезок.

ПРИМЕЧАНИЕ 2. – Аутентификатор вычисляется только по **ClearToken**.

ПРИМЕЧАНИЕ 3. – Должен использоваться метод дополнения битами внутри стандарта SHA1 (ИСО/МЭК 10118-3)

ПРИМЕЧАНИЕ 4. – Для того чтобы предупредить возможность атак воспроизведения, строго рекомендуется гарантировать в реализациях, чтобы пароль (ключ) менялся перед изменением (или завершением цикла) числа монотонно возрастающей последовательности.

ПРИМЕЧАНИЕ 5. – Получатель способен обнаружить использование процедуры IA путем оценки **OID** "B" внутри **tokenOID**.

Аутентификатор должен вычисляться только по **ClearToken** в **CryptoH323Token** (т. е. **ClearToken**) поля **token** поля **cryptoHashedToken**. Криптографический хэш должен вычисляться по шифрованной ASN.1 битовой строке **ClearToken**.

Конечные точки версии 1 и версии 2 H.235 могут использовать "только аутентификацию", в случае которой должны использоваться соответствующие OID для "B". Для конечных точек версии 1 H.235 необходимо придерживаться процедуры, описанной в пункте 11.

9 Иллюстрация использования для процедуры I

На рис. с 1 по 3 изображено присутствие общих ключей на конце каналов связи для различных комбинаций каналов привратника и прямой маршрутизации H.225.0. Независимо от модели вызова, секретный ключ всегда присутствует между конечной точкой и ее привратником для того, чтобы обеспечить аутентификацию и целостность сообщений RAS. Когда канал RAS и канал H.225.0 завершаются между двумя аналогичными узлами, можно использовать единый ключ для обеспечения аутентификации и целостности сообщений как RAS, так и H.225.0.

На рис. 1 показан самый масштабируемый сценарий, где обе конечные точки находятся внутри зон, в которых применяется модель с маршрутизацией привратником. Все участвующие привратники обоюдно совместно используют ключи. Сценарий, изображенный на рис. 1, рекомендуется для масштабируемости.

ПРИМЕЧАНИЕ 1. – Этот сценарий не обеспечивает достоверной сквозной защиты между конечными точками; вся защита зависит от доверенных промежуточных привратников.

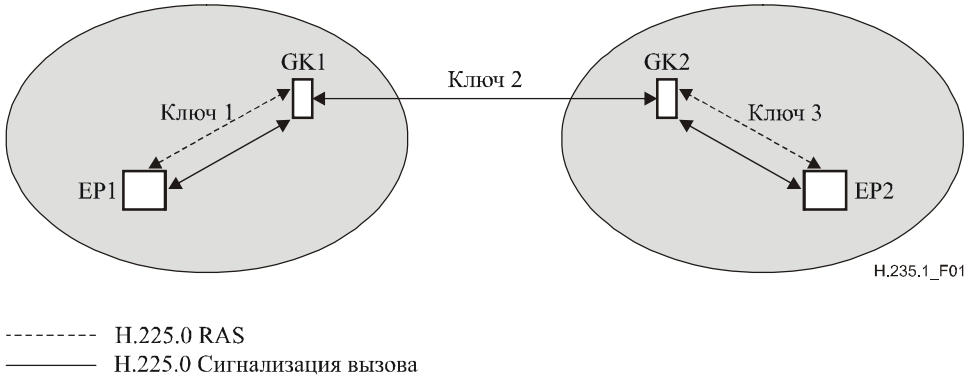
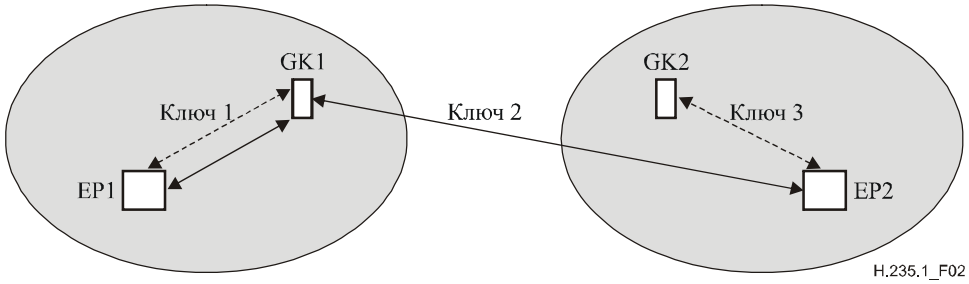


Рисунок 1/H.235.1 – Иллюстрация использования процедуры I в сценарии привратник–привратник с конечными точками, находящимися в зонах с маршрутизацией привратником

На рис. 2 показан смешанный сценарий, где одна конечная точка находится внутри зоны, в которой применяется модель с маршрутизацией привратником, в то время как другая конечная точка находится в зоне, в которой применяется модель с прямой маршрутизацией. Этот сценарий мог бы возникать в закрытых средах, где число конечных точек 2 и привратников 1 ограничено.

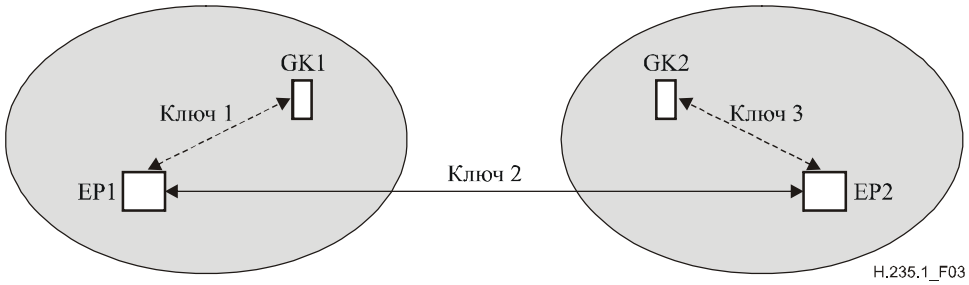


--------- H.225.0 RAS
———— H.225.0 Сигнализация вызова

Рисунок 2/H.235.1 – Иллюстрация использования процедуры I в смешанном сценарии с конечной точкой 1 в зоне с маршрутизацией привратником и конечной точкой 2 в зоне с прямой маршрутизацией

На рис. 3 показан сценарий, где обе конечные точки находятся внутри зон, в которых применяется модель с прямой маршрутизацией привратником. Этот сценарий не очень масштабируем, когда участвует много конечных точек. В принципе, вместо него рекомендуется использование H.235.2 с процедурами II/III. Для этого специфического сценария и процедур I, II или III необходимы также дополнительные меры защиты (защищающие против подмены и неправильного использования вызова, например, средствами авторизации вызова с метками доступа в шлюзах H.323), которые не описаны в этой Рекомендации; они будут изучены далее.

ПРИМЕЧАНИЕ 2. – В этом сценарии обеспечивается достоверная сквозная защита среди конечных точек, не полагающихся на доверенные промежуточные узлы.



--------- H.225.0 RAS
———— H.225.0 Сигнализация вызова

Рисунок 3/H.235.1 – Иллюстрация использования процедуры I в сценарии с конечными точками, обеими находящимися в зонах, в которых используется прямая маршрутизация привратником

Рассмотрим случай на рис. 1, где три пароля попарно совместно используются конечной точкой 1-привратником 1, привратником 1-привратником 2 и привратником 2-конечной точкой 2. Три 20-байтных ключа – *Ключ 1*, *Ключ 2* и *Ключ 3* – генерируются из этих паролей на основе процедуры, описанной в 8.2.4/H.235.0. Для достижения максимальной защиты рекомендуется сделать каждый из трех случайных паролей/ключей независимым.

Ниже, мы иллюстрируем подробности процедуры для аутентификации и целостности сообщений RAS, H.225.0 и H.245. В примере описания изображены специфические параметры в модели с маршрутизацией привратником; также возможны другие полезные и действенные комбинации идентификаторов объектов в других сценариях.

ПРИМЕЧАНИЕ 3. – Сценарии, показанные на рис. с 1 по 3, не масштабируются правильно в случае, где число общих симметричных ключей (паролей) для привратников (рис. 1), для привратников и удаленных конечных точек (рис. 2), или для конечных точек (рис. 3) становится слишком большим.

9.1 Аутентификация и целостность сообщений RAS

Рассмотрим случай, где конечная точка 1 желает послать сообщение RAS, скажем, сообщение **ARQ**, привратнику 1. Конечная точка 1 генерирует временную отметку и число последовательности и включает их в поля **timeStamp** и **random** соответственно, наряду с псевдонимом привратника 1 в **generalID** и ID конечной точки в поле **sendersID**. Эти поля присутствуют в поле **ClearToken** в **hashedVals**, присутствующем в **cryptoHashedToken** поля **CryptoToken** в **cryptoH323Token** сообщения **ARQ**.

tokenOID внутри **cryptoHashedToken** устанавливается в "A", это показывает, что все поля в сообщении **ARQ** хэшированы. **HASHED** внутри **token** в **cryptoHashedToken** содержит **algorithmOID**, установленный в "U", что показывает использование HMAC-SHA1-96 и **params** установленный в NULL. Конечная точка 1 затем вычисляет аутентификатор на основе HMAC-SHA1-96, используя 20-байтовый *Ключ 1*. Аутентификатор вычисляется по всему сообщению RAS.

Конечная точка 1 включает вычисленный аутентификатор внутрь **hash** в поле **token** поля **cryptoHashedToken** в **CryptoToken**, присутствующем в **cryptoH323Token** сообщения **ARQ**. Затем сообщение **ARQ** посылается привратнику 1.

При получении сообщения **ARQ**, привратник 1 проверяет аутентификатор на основе нескольких критериев, которые включают:

- живучесть **timestamp**, уникальность **random**;
- идентичность **generalID** и собственного идентификатора;
- совпадение аутентификатора сообщения **ARQ** с вычисленным привратником 1.

9.2 Аутентификация и целостность сообщений H.225.0

Рассмотрим случай, где конечная точка 1 желает послать сообщение H.225.0, скажем, сообщение **Setup** конечной точке 2. Конечная точка 1 генерирует временную отметку и число последовательности и включает их в поля **timeStamp** и **random** соответственно, наряду с псевдонимом привратника 1 в **generalID** и ID конечной точки в поле **sendersID**. Конечная точка 1 вычисляет также половину ключа Диффи-Хеллмана и включает параметры Диффи-Хеллмана **halfkey**, **modsize** и **generator** в поле **dhkey** в **ClearToken**. Эти поля присутствуют в поле **ClearToken** в **hashedVals**, присутствующем в **cryptoHashedToken** поля **CryptoToken** в **cryptoH323Token** сообщения **Setup**.

TokenOID внутри **cryptoHashedToken** установлен в "A", это показывает, что все поля в сообщении сигнализации H.225.0 хэшированы. **HASHED** внутри **token** в **cryptoHashedToken** содержит **algorithmOID**, установленный в "U", что показывает использование HMAC-SHA1-96 и **params**, установленный в NULL. Конечная точка 1 затем вычисляет аутентификатор на основе алгоритма HMAC-SHA1, используя 20-байтовый *Ключ 1*. Аутентификатор вычисляется согласно выбранному методу хэша (A) при взятии в расчет всего целиком сообщения сигнализации вызова H.225.0.

Конечная точка 1 включает вычисленный аутентификатор внутрь **hash** в поле **token** поля **cryptoHashedToken** в **CryptoToken**, присутствующего в **cryptoH323Token** сообщения **Setup**. Затем сообщение **Setup** посылается привратнику 1.

При получении сообщения **Setup**, привратник 1 проверяет аутентификатор на основе нескольких критериев, которые включают:

- живость **timestamp**, уникальность **random**;
- идентичность **generalID** и собственного идентификатора;
- проверка параметров Диффи-Хеллмана, например, тестирование, корректны ли 1024-битная основная часть и генератор. Тестирование того, безопасны ли параметры Диффи-Хеллмана, является процессом, отнимающим много времени и может осуществляться, только если того требуют локальные правила;
- совпадение аутентификатора в сообщении **Setup** с вычисленным привратником 1.

Если проверка аутентификатора прошла успешно, привратник 1 вычисляет новый аутентификатор чтобы вставить (заменить) в сообщение **Setup**, перед отправкой его в привратник 2, как следует далее. Привратник 1 заменяет поля **timeStamp**, **random**, **sendersID** и **generalID** в поле **ClearToken** поля **hashedVals**, используя значения, относящиеся к отрезку привратник 1-привратник 2. Поле **timestamp** содержит текущую временную отметку, поле **random** содержит следующее число монотонно возрастающей последовательности для отрезка привратник 1-привратник 2, поле **generalID** содержит псевдоним привратника 2 и **sendersID** содержит псевдоним привратника 1. Привратник 1 включает также полученные параметры Диффи-Хеллмана в поле **dhkey** поля **ClearToken**.

Привратник 1 затем вычисляет новый аутентификатор для этого сообщения сигнализации вылова H.225.0, используя *Ключ 2* и алгоритм HMAC-SHA1-96 (**algorithmOID**="U"), вставляет его в **hash** внутри **token** и передает сообщение **Setup** дальше к привратнику 2.

При получении сообщения **Setup** привратник 2 проверяет аутентификатор, вычисляет новый аутентификатор после соответствующего видоизменения полей **ClearToken** в **hashedVals**, вставляет его в поле **hash** и передает сообщение **Setup** дальше к конечной точке 2.

9.3 Аутентификация и целостность сообщений H.245

Рассмотрим случай, где конечная точка 1 желает послать сообщение H.245, скажем, сообщение **TerminalCapabilitySet**, конечной точке 2. Конечная точка 1 выясняет, необходимо ли послать сообщение H.225.0 привратнику 1. Если так, то сообщение H.245 туннелируется внутрь того сообщения H.225.0. Поля внутри сообщения H.225.0 устанавливаются, как описано ранее, на передачу сообщения H.225.0. Так как сообщение H.245 туннелировано, **h323-uu-pdu** в сообщении **h323-UserInformation** имеет свои поля, установленные следующим образом:

- поле **h323-message-body** установлено на тип сообщения H.225.0, которое передается.
- **h245Tunnelling** установлено в TRUE.
- **h245Control** содержит строку октетов H.245 PDU.

Конечная точка 1 генерирует **CryptoToken** для сообщения H.225.0, устанавливает **tokenOID** в "A", что показывает аутентификацию и целостность, устанавливает **timeStamp**, **random**, **sendersID**, **generalID** и **tokenOID** в "T" в **ClearToken** поля **hashedVals**, устанавливает **algorithmOID** в "U", что показывает использование HMAC-SHA1-96 и **hash** на вычисленный аутентификатор хэша по всем полям сообщения сигнализации вызова H.225.0.

Однако, если передачи сообщения H.225.0 не ожидается, то сообщение H.245 туннелируется внутрь специально созданного для данного случая сообщения **facility** H.225.0. **h323-uu-pdu** в сообщении **h323-UserInformation** имеет свои поля, установленные следующим образом:

- поле **h323-message-body** установлено в **facility**, которое содержит:
  - **reason**, установленное в **undefinedReason**;
  - **tokens** и **cryptoTokens** установленные как для любого сообщения H.225.0.
- **h245Tunnelling** установлено в TRUE.
- **h245Control** содержит строку октетов H.245 PDU.

Как описано выше, конечная точка 1 генерирует **CryptoToken** как часть сообщения **facility** H.225.0. Сообщение **facility** затем передается конечной точкой 1 привратнику 1.

В каждом из случаев (ожидается ли передача сообщения H.225.0 или используется специально созданное для этого случая сообщение **facility** H.225.0), привратник 1 проверяет аутентификатор при получении сообщения. Затем, если ожидается передача сообщения H.225.0 по отрезку привратник 1-привратник 2, сообщение H.245 туннелируется внутрь этого сообщения; иначе, оно туннелируется внутрь специально созданного для этого случая сообщения **facility** H.225.0. Как в случае передачи любого сообщения H.225.0, вычисляется новый аутентификатор для сообщения H.225.0 перед его передачей привратником 1 привратнику 2. Процесс повторяется для отрезка привратник 2-конечная точка 2.

9.4 Сценарий с прямой маршрутизацией

Защищенные объекты H.323 могут связываться не только внутри среды, маршрутизируемой привратником, как обозначено в этой Рекомендации, но могут также использовать модель прямой маршрутизации. Эта модель прямой маршрутизации требует дополнительные меры защиты (метки доступа), в которых нет необходимости в более простых средах с маршрутизацией привратником. Рек. МСЭ-Т H.235.4 описывает как защитить модели с прямой маршрутизацией.

10 Поддержка серверных служб

Защищенные объекты H.323 могут пользоваться услугами серверных служб, согласно процедуре, описанной в I.1.6/H.235.0.

11 Совместимость с версией 1 H.235

Несмотря на то, что эти профили защиты разрабатываются совместно с версией 2 Рек. МСЭ-Т H.235 (Рек. МСЭ-Т H.235 (2000 г.)) подразумевается, что также возможно применять профили защиты для версии 1 Рек. МСЭ-Т H.235 (Рек. МСЭ-Т H.235 (1998 г.)) с некоторыми незначительными изменениями. Получатель способен обнаружить присутствие версии протокола H.235 отправителя посредством оценки идентификаторов объектов профиля защиты (см. пункт 15).

Реализации Версии 1 Рек. МСЭ-Т H.235 (Рек. МСЭ-Т H.235 (1998 г.)):

- не устанавливают или оценивают **sendersID** в **ClearToken**.
- не используют услуги серверных служб, как в пункте 10.

12 Многоадресный режим

Многоадресные сообщения H.225.0, такие как GRQ или LRQ не должны включать CryptoToken согласно процедуре I. Когда такие сообщения посылаются как одноадресные, сообщение должно включать CryptoToken.

13 Список защищенных сообщений сигнализации

В этом пункте предоставлены общие сведения о том, как и какими средствами в данной Рекомендации обеспечивается защита различных сообщений сигнализации H.323.

13.1 H.225.0 RAS

Сообщение RAS H.225.0	Поля сигнализации H.235	Аутентификация и целостность
Любое	cryptoTokens	Процедура I

13.2 Сигнализация вызова H.225.0

Сообщение сигнализации H.225.0	Поля сигнализации H.235	Аутентификация и целостность
Alerting-UUIE, CallProceeding-UUIE, Connect-UUIE, Setup-UUIE, Facility-UUIE, Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	cryptoTokens	Процедура I

13.3 Контроль вызова H.245

Сообщения H.245 "в" и "из" защищенных объектов H.323 должны либо быть совмещены при передаче прямых и обратных пакетов как часть защищенного быстрого соединения (fast-connect), либо должны быть туннелированы с использованием защищенного **Facility-UUIE** H.225.0.

14 Использование sendersID и generalID

ClearToken содержит поля **sendersID** и **generalID**. Когда информация идентификации доступна, **sendersID** должен быть установлен на идентификатор привратника (GKID) для сообщения, инициированного привратником и на идентификатор конечной точки (EPID) для сообщений, инициированных конечной точкой. Когда информация идентификации доступна, **generalID** должен быть установлен на GKID) для сообщений, инициированных конечной точкой и на EPID для сообщений, инициированных привратником. Когда информация идентификации не доступна, или в случае вещания/многоадресной рассылки является неоднозначной, поле отсутствует или должно содержать нулевую строку. В таблице 2 подводится итог по данной информации.

Таблица 2/H.235.1 – Использование sendersID и generalID

Сообщение	sendersID	generalID
Одноадресное **GRQ**	**EPID** если доступна, иначе **NULL**	**GKID**
Многоадресное **GRQ**	**EPID** если доступна, иначе **NULL**	
GCF, **GRJ**	**GKID**	**EPID** если доступна, иначе **NULL**
Первоначальное **RRQ**	**EPID** если доступна, иначе **NULL**	**GKID**
RCF	**GKID**	**EPID**
RRJ	**GKID**	
URQ, **UCF**, **URJ**, **BRQ**, **BCF**, **BRJ**, **DRQ**, **DCF**, **DRJ**, **NSM**, **RIP**, **SCI**, **SCR**, **XRS (EP-to-GK)**	**EPID**	**GKID**
URQ, **UCF**, **URJ**, **BRQ**, **BCF**, **BRJ**, **DRQ**, **DCF**, **DRJ**, **NSM**, **RIP**, **SCI**, **SCR**, **XRS (GK-to-EP)**	**GKID**	**EPID**
ARQ, **IRQ**, **RAI**	**EPID**	**GKID**
ACF, **ARJ**, **BCF**, **LCF**, **LRJ**, **IRR**, **IRQ**, **RAC**, **LCF**, **LRJ**, **IACK**, **INAK**	**GKID**	**EPID**
Одноадресное **LRQ** (конечная точка–привратник)	**EPID**	**GKID**
Одноадресное **LRQ** (привратник–привратник)	**GKID**	**GKID**
Многоадресное **LRQ**	**EPID**	
ПРИМЕЧАНИЕ. – GKID обозначает идентификатор привратника, EPID обозначает идентификатор конечной точки. Пустое поле обозначает отсутствие или нулевую строку идентификации.		

15 Список идентификаторов объектов

В таблице 3 перечислены все упомянутые OID (см. также [OIW] и [WEBOIDs]). Существуют идентификаторы объектов для H.235v1 и для H.235v2.

Таблица 3/H.235.1 – Идентификаторы объекта

Ссылка на идентификатор объекта	Значение(я) идентификатора объекта	Описание
"A"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 1} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 1}	Используется в процедуре I для CryptoToken-tokenOID, показывая, что хэш включает все поля в RAS H.225.0 и сообщении сигнализации вызова (аутентификация и целостность).
"E"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 9} {itu-t (0) recommendation (0) h (8) 235 version (0) 2 9}	Сквозной ClearToken, несущий sendersID для проверки на стороне получателя
"T"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 5} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 5}	Используется в процедурах I и IA как базовый ClearToken для аутентификации сообщений и защиты от атак воспроизведения и дополнительно для управления ключом Диффи-Хеллмана, как описано в пункте 8.5/H.235.6
"U"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 6} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 6}	Используется в процедуре I для Algorithm OID, показывая использование HMAC-SHA1-96.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	**Аудиовизуальные и мультимедийные системы**
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2007 г.