МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

H.235.0

(09/2005)

СЕРИЯ H: АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

Инфраструктура аудиовизуальных услуг – Системные аспекты

Защита H.323: Инфраструктура защиты в мультимедийных системах серии H (H.323 и других, основанных на H.245)

Рекомендация МСЭ-Т H.235.0

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.235.0

Защита H.323: Инфраструктура защиты мультимедийных систем серии H (H.323 и других, основанных на H.245)

Резюме

В данной Рекомендации описываются улучшения в инфраструктуре Рекомендаций серий H.3xx, для того чтобы внедрить такие услуги защиты, как *аутентификация* и *секретность* (шифрование данных). Предложенная схема применима как к простым конференциям точка-точка, так и к многоточечным конференциям, для любых оконечных устройств, использующих Рек. МСЭ-Т H.245 в качестве протокола контроля; а также для систем H.323, использующих RAS H.225.0 и/или протокол сигнализации вызова.

Например, системы H.323 работают через сети, основанные на передаче пакетов, которые не обеспечивают гарантированное качество обслуживания. По тем же техническим причинам, по которым базовая сеть не обеспечивает качество обслуживания, сеть не обеспечивает услуги защиты. Конфиденциальная связь в режиме реального времени по незащищенным сетям обычно включает две основных области проблем – а*утентификацию* и *секретность*.

В данной Рекомендации описана инфраструктура защиты и конкретные методы секретности, используемые в мультимедийных системах серий H.3xx. В данной Рекомендации раскрыты области проблем, касающиеся интерактивных конференций. Эти области включают, но не строго ими ограничиваются, аутентификацию и секретность всех потоков медиа в режиме реального времени, обмен которыми происходит при конференции. В данной Рекомендации предоставлены протокол и алгоритмы, необходимые для реализации между объектами серии H.323.

В данной Рекомендации использованы общие средства, поддерживаемые в Рек. МСЭ-Т H.245, и, по существу, в любом стандарте, работающем совместно с этим протоколом контроля, можно использовать эту инфраструктуру защиты. Ожидается, что по возможности другие оконечные устройства серии H смогут взаимодействовать и непосредственно использовать методы, описанные в этой Рекомендации. Изначально не будет предусмотрена полная реализация этой Рекомендации во всех областях, в ней особенно будут выделены аутентификация конечных точек и секретность медиа.

В данную Рекомендацию включена возможность согласования услуг и выполняемых функций в общем смысле и возможность выбора криптографических методов и используемых возможностей. Конкретный метод их использования связан с возможностями систем, требованиями к применению и конкретными ограничениями политики защиты. В данной Рекомендации поддерживаются различные криптографические алгоритмы с разными вариантами, подходящими для различных целей; например, длинами ключа. Конкретные криптографические алгоритмы могут распределяться специфическим услугам защиты (например, один для скоростного шифрования потока медиа, а другой для шифрования сигнализации).

Следует также заметить, что некоторые из доступных криптографических алгоритмов или механизмов могут быть зарезервированы для экспорта или других национальных действий (например, с ограниченными длинами ключа). В данной Рекомендации поддерживается сигнализация хорошо известных алгоритмов в дополнение к нестандартизованной сигнализации или патентованных криптографических алгоритмов. В ней не содержится конкретных обязательных алгоритмов; однако строго рекомендуется, чтобы конечные точки поддерживали столько применимых алгоритмов, сколько возможно для достижения возможности взаимодействия. Это аналогично концепции о том, что поддержка Рек. МСЭ-Т H.245 не гарантирует функциональную совместимость между кодеками двух объектов.

Версия 4 Рек. МСЭ-Т H.235 разделяет бывшую Рек. МСЭ-Т H.235v3 на набор Рекомендаций подсерии H.235.x и реструктурирует подсерию. В набор добавлены новые Рекомендации МСЭ-Т H.235.8 и H.235.9; другие Рекомендации подсерии расширены новыми выполняемыми функциями (Рекомендации МСЭ-Т H.235.3, H.235.5). В Рек. МСЭ-Т H.235.0 содержится инфраструктура защиты H.323 с общим текстом и полезной общей информацией для всех Рекомендаций подсерии H.235.x.

В новых Приложениях IV, V, и VI H.235.0 содержится текст, иллюстрации и таблицы из Рек. МСЭ-Т H.235 версии 3 (2003 г.), включая последующие Исправление 1 и поправки для новой структуры.

Источник

Рекомендация МСЭ-Т H.235.0 утверждена 13 сентября 2005 г. 16-й Исследовательской комиссией МСЭ-Т (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.

СОДЕРЖАНИЕ

		Стр.
1	Сфера применения	1
1.1	Структура Рекомендаций подсерии H.235.x	2
2	Справочные документы	2
2.1	Нормативные справочные документы	2
2.2	Информативные справочные документы	4
3	Термины и определения	4
4	Символы и сокращения	6
5	Соглашения по терминам	7
6	Введение в систему	8
6.1	Резюме	9
6.2	Аутентификация	9
6.3	Защита установления вызова	10
6.4	Защита контроля вызова (H.245)	10
6.5	Секретность потока медиа	10
6.6	Защитные элементы	11
6.7	Невозможность отказа	11
6.8	Конфиденциальность подвижной связи	12
6.9	Профили защиты	12
6.10	Прохождение через защищенные NAT/сетевые экраны	13
7	Процедуры осуществления соединения	13
8	Сигнализация и процедуры аутентификации	14
8.1	Схема Диффи-Хеллмана с дополнительной аутентификацией	14
8.2	Аутентификация на основе подписей	15
8.3	Сигнализация/процедуры RAS для аутентификации	19
8.4	Управление ключом в канале RAS	22
9	Ассиметричная аутентификация и обмен ключами с использованием систем шифрования эллиптической кривой	23
9.1	Управление ключом	23
9.2	Цифровая подпись	23
10	Псевдослучайная функция (PRF)	23
11	Восстановление при ошибках защиты	24
11.1	Сигнализация ошибок	24
Приложение A – H.235 ASN.1		26
Приложение B – Особые вопросы H.324		31
Дополнение I – Подробности реализации в H.323		31
I.1	Примеры реализации	31
Дополнение II – Подробности реализации в H.324		36
Дополнение III – Другие подробности реализации серии H		36

Стр.

Дополнение IV – Соответствие разделов H.235v3Amd1Cor1 подсерии Рекомендаций H.235v4 37

Дополнение V – Соответствие рисунков H.235v3Amd1Cor1 подсерии Рекомендаций H.235v4 45

Дополнение VI – Соответствие таблиц H.235v3Amd1Cor1 подсерии Рекомендаций H.235v4 48

Рекомендация МСЭ-Т H.235.0

Защита H.323: Инфраструктура защиты в мультимедийных системах серии H (H.323 и других, основанных на H.245)

1 Сфера применения

Основная цель данной Рекомендации заключается в предоставлении инфраструктуры защиты для аутентификации, секретности и целостности внутри нынешней инфраструктуры протокола серии H. В настоящем тексте этой Рекомендации содержатся подробности реализации Рек. МСЭ-Т H.323. Предполагается, что эта инфраструктура будет работать совместно с другими протоколами серии H, использующими Рек. МСЭ-Т H.245 в качестве протокола контроля и/или использующими RAS H.225.0 и/или протокол сигнализации вызова.

Дополнительные цели данной Рекомендации включают:

1) Архитектура защиты должна разрабатываться как расширяемая и гибкая инфраструктура для реализации системы защиты в оконечных устройствах серии H и других основанных на H.323 системах. Это следует обеспечить посредством гибких и независимых услуг и предоставляемых ими функций. Сюда включена возможность согласования и выбора используемых криптографических методов и способа их использования.

2) Обеспечение конфиденциальности всех связей, возникающих как результат использования протокола H.3xx. Сюда включены аспекты установления соединения, контроля вызова и обмена медиа между всеми объектами. Это требование включает использование конфиденциального соединения (секретности) и может использовать функции равноправной аутентификации, а также защиты пользовательской среды от атак.

3) В этой Рекомендации не должны создаваться препятствия интеграции других функций защиты в объектах H.3xx, которые могут защитить их от сетевых атак.

4) В этой Рекомендации не должны создаваться ограничения возможностям надлежащего масштабирования Рекомендаций серии H.3xx. Это может включать как число защищенных пользователей, так и уровни предоставленной защиты.

5) Когда это уместно, все механизмы и средства должны быть предоставлены независимыми от любой лежащей в основе передачи или топологии. Для противостояния подобным угрозам могут потребоваться другие методы, лежащие выходящие за рамки области применения данной Рекомендации.

6) Положения созданы для работы в смешанных средах (защищенные и незащищенные объекты).

7) В данной Рекомендации должны быть предусмотрены средства для распространения сеансовых ключей, относящихся к используемому шифрованию. (Это не подразумевает, что частью этой Рекомендации должно быть управление сертификатами на основе шифрования открытым ключом.)

8) В данной Рекомендации предусмотрено два профиля защиты, которые упрощают функциональную совместимость. В H.235.1 описан простой, тем не менее надежный профиль защиты, основанный на пароле, а в H.235.2 – профиль защиты, использующий цифровые подписи, сертификаты и инфраструктуру открытого ключа, в котором преодолены ограничения H.235.1.

Архитектура защиты, описанная в данной Рекомендации, не предполагает, что участники знакомы друг с другом. Она, однако, предполагает, что были приняты надлежащие меры предосторожности, чтобы физически защитить конечные точки серии H. Следовательно, предполагается, что основная угроза защиты для соединений заключается в прослушивании через сеть или каком-либо другом методе отвода информационных потоков.

В Рек. МСЭ-Т H.323 предусмотрены средства проведения аудио-, видео- и информационных конференций между двумя и более сторонами, но не предусмотрен механизм, позволяющий каждому участнику устанавливать подлинность других участников, как и не предусмотрены средства, для того чтобы сделать соединения частными (т. е. шифровать потоки).

В Рекомендациях МСЭ-Т H.323, H.324 и H.310 используются процедуры сигнализации логического канала Рек. МСЭ-Т H.245, в которой содержимое каждого логического канала описывается, когда канал открыт. Процедуры предусмотрены для представления возможностей приемника и передатчика, передачи ограничены тем, что могут расшифровать приемники, и приемники могут запросить определенный желательный режим у передатчиков. Возможности защиты каждой конечной точки связаны таким же образом, как и любая другая возможность связи.

Некоторые оконечные устройства серии H (H.323) могут быть использованы в многоточечных конфигурациях. Механизм защиты, описанный в этой Рекомендации, позволит достичь конфиденциального функционирования в этих средах, включая как централизованное, так и децентрализованное функционирование MCU.

1.1 Структура Рекомендаций подсерии H.235.x

Данная Рекомендация по инфраструктуре защиты охватывает следующую структуру внутри подсерии H.235.x Рекомендаций, показанную на рисунке 1. В этой Рекомендации содержится общий текст и полезная общая информация для всех Рекомендаций подсерий H.235.x.

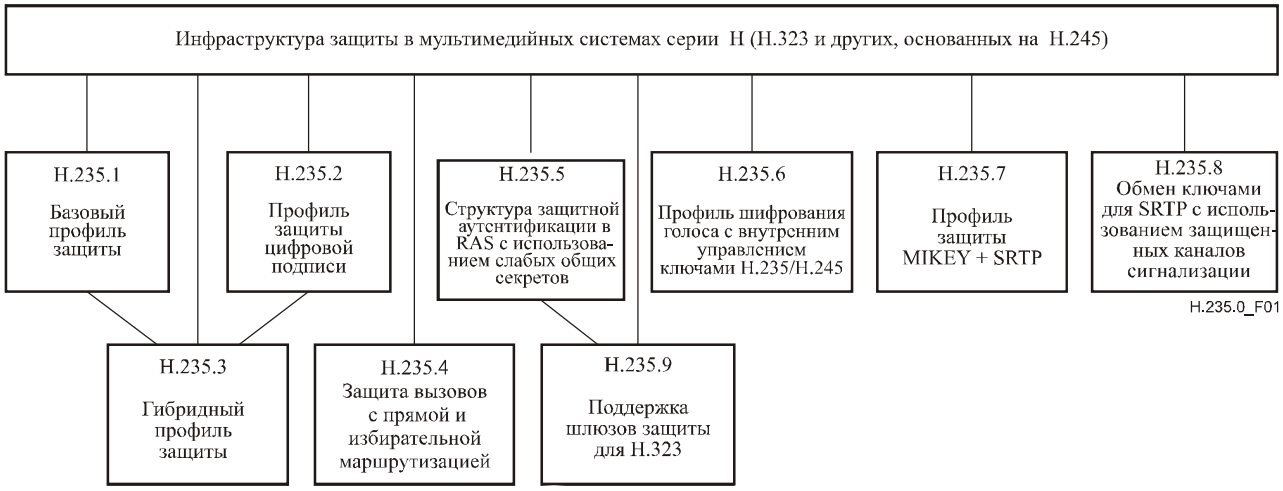


Рисунок 1/H.235.0 – Структура Рекомендаций подсерий H.235.x

Вертикальными линиями на рисунке 1 показана прямая зависимость от главного текста H.235.0; могут быть и другие непрямые зависимости от других Рекомендаций H.235.x. Некоторые Рекомендации можно использовать в сочетании друг с другом и дополняя друг друга, см. также 6.9.

2 Справочные документы

2.1 Нормативные справочные документы

В перечисленных ниже Рекомендациях МСЭ-Т и других справочных документах 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 другие справочные документы являются предметом корректировки, в связи с чем пользователям данной Рекомендации настоятельно рекомендуется изыскать возможность для использования самых последних изданий Рекомендации и справочных документов, перечисленных ниже. Регулярно публикуется перечень действующих Рекомендаций МСЭ-Т. Ссылка на документ в рамках этой Рекомендации не дает ему, как отдельному документу, статуса рекомендации.

– ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

– ITU-T Recommendation H.235 (2003), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals* plus Amendment 1 (2004), plus Corrigendum 1 (2005).

– ITU-T Recommendation H.235.1 (2005), *H.323 security: Baseline security profile*.

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

– ITU-T Recommendation H.235.3 (2005), *H.323 security: Hybrid security profile*.

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

– ITU-T Recommendation H.235.5 (2005), *H.323 security: Framework for secure authentication in RAS using weak shared secrets*.

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

– ITU-T Recommendation H.235.7 (2005), *H.323 security: Usage of the MIKEY key management protocol for the Secure Real Time Transport Protocol (SRTP) within H.235*.

– ITU-T Recommendation H.235.8 (2005), *H.323 security: Key exchange for SRTP using secure signalling channels*.

– ITU-T Recommendation H.235.9 (2005), *H.323 security: Security gateway support for H.323*.

– ITU-T Recommendation H.245 (2005), *Control protocol for multimedia communication*.

– ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems*.

– ITU-T Recommendation H.530 (2002), *Symmetric security procedures for H.323 mobility in H.510,* plus Corrigendum 1 (2003).

– 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 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 9798-2:1999, *Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms*.

– ISO/IEC 9798-3:1998, *Information technology – Security techniques – Entity authentication – Part 3: Mechanism using digital signature techniques*.

– ISO/IEC 9798-4:1999, *Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function*.

– ISO/IEC 15946-1:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General*.

– ISO/IEC 15946-2:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures*.

– ATM Forum: af-sec-0100.002 (2001), *ATM Security Specification Version 1.1*.

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

– IETF RFC 2407 (1998), *The Internet IP Security Domain of Interpretation for ISAKMP*.

– IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*.

– IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*.

– IETF RFC 3546 (2003), Transport Layer Security Protocol (TLS) Extensions.

– IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing*.

2.2 Информативные справочные документы

[Daemon] DAEMON (J.), *Cipher and Hash function design*, Ph.D. Thesis, Katholieke Universiteit Leuven, March 1995.

[ESP] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*.

[OAKLEY] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*.

[IKE] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

[ISO|IEC 14888-3] ISO/IEC 14888-3:1998, *Information technology – Security techniques – Digital signatures with appendix; Part 3: Certificate-based mechanisms*.

[J.170] ITU-T Recommendation J.170 (2005), *IPCablecom security specification*.

[RTP] IETF RFC 3550 (2003), *RTP: A transport Protocol for Real-Time Applications*.

[Schneier] SCHNEIER (B.), *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley & Sons, Inc., 1995.

[SRTP] IETF RFC 3711 (2004), *The Secure Real-Time Transport Protocol (SRTP)*.

3 Термины и определения

Согласно целям этой 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 следующих терминов, используемых в этой Рекомендации, также определены в Рекомендациях МСЭ-Т X.800 | ИСО 7498-2, X.803 | ИСО/МЭК 10745, X.810 | ИСО/МЭК 10181-1 и X.811 | ИСО/МЭК 10181-2.

3.1 контроль доступа: Предупреждение неавторизованного использования ресурса, включая предупреждение использования ресурса неавторизованным способом (Рек. МСЭ-Т X.800).

3.2 аутентификация: Предоставление гарантий заявленной подлинности объекта (Рек. МСЭ-Т X.811 | ИСО/МЭК 10181-2).

3.3 авторизация: Предоставление разрешения на основе пройденной аутентификации.

3.4 атака: Действия, предпринятые с целью обойти или воспользоваться слабыми местами в системных механизмах защиты. Посредством прямой атаки системы они используют слабые места в алгоритмах, принципах и свойствах, лежащих в основе механизма защиты. Непрямая атака происходит, когда они обходят механизм или когда они заставляют систему неправильно использовать механизм.

3.5 сертификат: Набор защищенных данных, выпущенных при авторизации системы защиты или третьей доверенной группой, наряду с информацией о защите, используемой для обеспечения целостности, и услугами установления подлинности данных (Рек. МСЭ-Т X.810 | ИСО/МЭК 10181-1). В этой Рекомендации данный термин относится к сертификатам "открытого шифровального ключа", являющимся значениями, которые представляют открытый ключ владельца (и другую

дополнительную информацию), будучи проверены и подписаны доверенным органом в неподдельном формате.

3.6 шифр: Криптографический алгоритм, математическое преобразование.

3.7 конфиденциальность: Свойство, не допускающее раскрытия информации неавторизованным личностям, объектам или процессам.

3.8 криптографический алгоритм: Математическая функция, значение которой вычисляется по одному или нескольким вводным значениям.

3.8 *bis* EC-GDSA: Цифровая подпись в виде эллиптической кривой с дополнительным аналогом алгоритма цифровой подписи (DSA) NIST (см. также ИСО/МЭК 15946-2, глава 5).

3.8 *ter* Система шифрования эллиптической кривой: Шифровальная система с открытым ключом (см. раздел 8.7 *ATM Forum Security Specification Version 1.1*).

3.8 *quat* Схема реализации соглашения с ключом эллиптической кривой – Диффи-Хеллман: Схема реализации соглашения с ключом Диффи-Хеллмана, использующая шифрование эллиптической кривой.

3.9 шифрование: Шифрование – это процесс преобразования данных в форму, нечитаемую неавторизованными объектами, с применением криптографического алгоритма. Дешифрование – это обратная операция, посредством которой шифрованный текст преобразуется в обычный текст.

3.10 целостность: Свойство, характеризующее данные, не измененные неавторизованным способом.

3.11 управление ключом: Генерация, хранение, распространение, удаление, архивация и применение ключей в соответствии с правилами защиты (Рек. МСЭ-Т X.800).

3.12 поток медиа: Поток медиа может иметь тип аудио, видео или данных или любой их комбинации. Данные потоков медиа переносят данные пользователей или приложений (полезные данные), но не контрольные данные.

3.13 невозможность отказа: Защита от отказа одного из объектов, вовлеченных в процесс передачи информации, в том, что он участвовал во всем процессе или в части этого процесса.

3.14 секретность: Режим связи, в котором только явно уполномоченные группы могут понимать друг друга. Это обычно достигается шифрованием и использованием общего ключа (ключей) для шифра.

3.15 частный канал: Для данной Рекомендации частный канал – это тот, который образуется в результате предварительного согласования на защищенном канале. В данном контексте он может использоваться для переноса потоков медиа.

3.16 шифрование открытым ключом: Система шифрования, использующая ассиметричные ключи (для шифрования/дешифрования), в которой ключи имеют математические соотношения друг с другом, которые нельзя вычислить явным способом.

3.17 профиль защиты: (Под)набор согласующихся, совместимых процедур и возможностей из Рек. МСЭ-Т H.235, полезных для обеспечения защиты мультимедийных коммуникаций H.323 среди вовлеченных объектов по специфическому сценарию.

3.18 спамминг: Атака отказа от обслуживания, при которой посылаются неавторизованные данные, перегружающие систему. Особый случай спамминга медиа: когда посылаются RTP пакеты на UDP порты. Обычно система переполняется пакетами; процесс потребляет большую часть системных ресурсов.

3.19 симметричный (основанный на секретном ключе) криптографический алгоритм: Алгоритм для выполнения шифрования или соответствующий алгоритм для выполнения дешифрования, в котором один и тот же ключ используется как для шифрования, так и для дешифрования (Рек. МСЭ-Т X.810 | ИСО/МЭК 10181-1).

3.20 угроза: Потенциальное нарушение защиты (Рек. МСЭ-Т X.800 | ИСО 7498-2).

4 Символы и сокращения

В этой Рекомендации используются следующие символы и сокращения:

X || Y	Concatenation of X and Y	Связь X и Y	
3DES	Triple DES	Тройной стандарт шифрования данных	
AES	Advanced Encryption Algorithm	Усовершенствованный алгоритм шифрования	
ALG	Application Layer Gateway	Шлюз прикладного уровня	
ASN.1	Abstract Syntax Notation One	Абстрактная синтаксическая нотация версии один	
BES	Back-end Server	Сервер служб	
CA	Certificate Authority	Орган сертификации	
CBC	Cipher Block Chaining	Блоковое сцепление шифра	
CFB	Cipher Feedback mode	Режим обратной связи по шифрованному тексту	
CRL	Certificate Revocation List	Список недействительных сертификатов	
DES	Data Encryption Standard	Стандарт шифрования данных	
DH	Diffie-Hellman	Диффи-Хеллман	
DNS	Domain Name System	Система наименования домен	
DSS	Digital Signature Standard	Стандарт цифровой подписи	
DTMF	Dual Tone Multi-Frequency	Двухтональный многочастотный	
ECB	Electronic Code Book	Электронная книга кодов	
ECC and EC	Elliptic Curve Cryptosystem (see section 8.7 of *ATM Forum Security Specification Version 1.1*). A public-key cryptosystem.	Система шифрования эллиптической кривой. Система шифрования открытым ключом	
EC-GDSA	Elliptic curve digital signature with appendix analog of the NIST Digital Signature Algorithm (DSA) (see also ISO/IEC 15946-2, chapter 5)	Цифровая подпись в виде эллиптической кривой с дополнительным аналогом алгоритма цифровой подписи (см. также ИСО/МЭК 15946-2, глава 5)	
ECKAS-DH	Elliptic Curve Key Agreement Scheme – Diffie-Hellman. The Diffie-Hellman key agreement scheme using elliptic curve cryptography	Схема реализации соглашения с ключом Диффи-Хеллмана, использующая шифрование эллиптической кривой	
EOFB	Enhanced OFB mode	Расширенный режим OFB	
EP	Endpoint	Конечная точка	
GK	Gatekeeper	Привратник	
GW	Gateway	Шлюз	
ICV	Integrity Check Value	Значение проверки целостности	
ID	Identifier	Идентификатор	
IETF	Internet Engineering Task Force	Целевая группа по инженерным проблемам интернета	
IPsec	Internet Protocol Security	Защита протокола Интернет	
ISAKMP	Internet Security Association Key Management Protocol	Протокол управления ключом ассоциации безопасности интернет	
ISO	International Organization for Standardization	Международная организация по стандартизации	ИСО
IV	Initialization Vector	Вектор инициализации	

LDAP	Lightweight Directory Access Protocol	Легковесный протокол доступа к справочнику
MAC	Message Authentication Code	Код аутентификации сообщения
MC	Multicast Controller	Многоадресный контроллер
MCU	Multipoint Control Unit	Блок управления многоточечной связью
MPS	Multiple Payload Stream	Групповой поток полезной нагрузки
NAT	Network Address Translation	Трансляция сетевого адреса
OCSP	Online Certificate Status Protocol	Онлайновый протокол статуса сертификата
OFB	Output Feedback Mode	Режим обратной связи выходных данных
OID	Object Identifier	Идентификатор объекта
PDU	Protocol Data Unit	Единица данных протокола
PKI	Public Key Infrastructure	Инфраструктура открытого ключа
POTS	Plain Old Telephone Service	Простая старая телефонная служба
PRF	Pseudo-Random Function	Псевдослучайная функция
Q&A	Question and Answer	Вопрос-ответ
QoS	Quality of Service	Обслуживания
RAS	Registration, Admission, Status	Допуск, статус
RSA	Rivest, Shamir and Adleman (public key algorithm)	Алгоритм шифрования открытым ключом
RTCP	Real-time Transport Control Protocol	Протокол управления передачей данных в режиме реального времени
RTP	Real-time Transport Protocol	Протокол передачи в режиме реального времени
SASET	Secure Audio Simple Endpoint Type	Конфиденциальный простой аудио тип конечной точки
SDU	Service Data Unit	Сервисный блок данных
SHA1	Secure Hash Algorithm 1	Алгоритм аутентификации и проверки целостности информации
SRTP	Secure Real-Time Transport Protocol	Конфиденциальный протокол передачи в режиме реального времени
SSL	Secure Socket Layer	Уровень защищенных сокетов
TLS	Transport Level Security	Защита транспортного уровня
TSAP	Transport Service Access Point	Точка доступа к услугам транспортного уровня
TTP	Trusted Third Party	Третья доверенная группа
UDP	User Datagram Protocol	Протокол дейтаграмм пользователя
XOR, ⊕	Exclusive OR	Исключающее ИЛИ

5 Соглашения по терминам

В этой Рекомендации используются следующие соглашения:

– "должен" указывает обязательное требование.

– "следует" указывает на предлагаемый, но не обязательный ход действий.

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

Ссылки на пункты, подпункты, дополнения и приложения внутри этой Рекомендации, кроме других Рекомендаций, изложены детально. К примеру, "1.4" указывает на пункт 1.4 этой Рекомендации; "6.4/H.245" указывает на пункт 6.4 в Рек. МСЭ-Т H.245.

В данной Рекомендации описывается использование "n" различных типов сообщений: H.245, RAS, Q.931 и т. д. Чтобы определить различия между разными типами сообщений, приводятся следующие соглашения. Сообщение и имена параметров H.245 состоят из сцепленных слов, выделенных жирным шрифтом (**maximumDelayJitter**). Имена сообщения RAS представлены аббревиатурами из трех букв (**ARQ**). Имена сообщения Q.931 состоят из одного или двух слов, начинающихся с заглавных букв (**Call Proceeding**).

В данной Рекомендации используется понятие установления структуры данных ASN.1 в NULL; к примеру, "**paramS** set to NULL" (см. пункт 7/H.235.1, пункт 8/H.235.1, 9.1/H.235.1, 9.2/H.235.1, пункт 7/H.235.2, пункт 9/H.235.2, 15.1/H.235.2 и 15.2/H.235.2). Это должно означать, что все дополнительные элементы, в особой ПОСЛЕДОВАТЕЛЬНОСТИ (т. е. **Params**) отсутствуют.

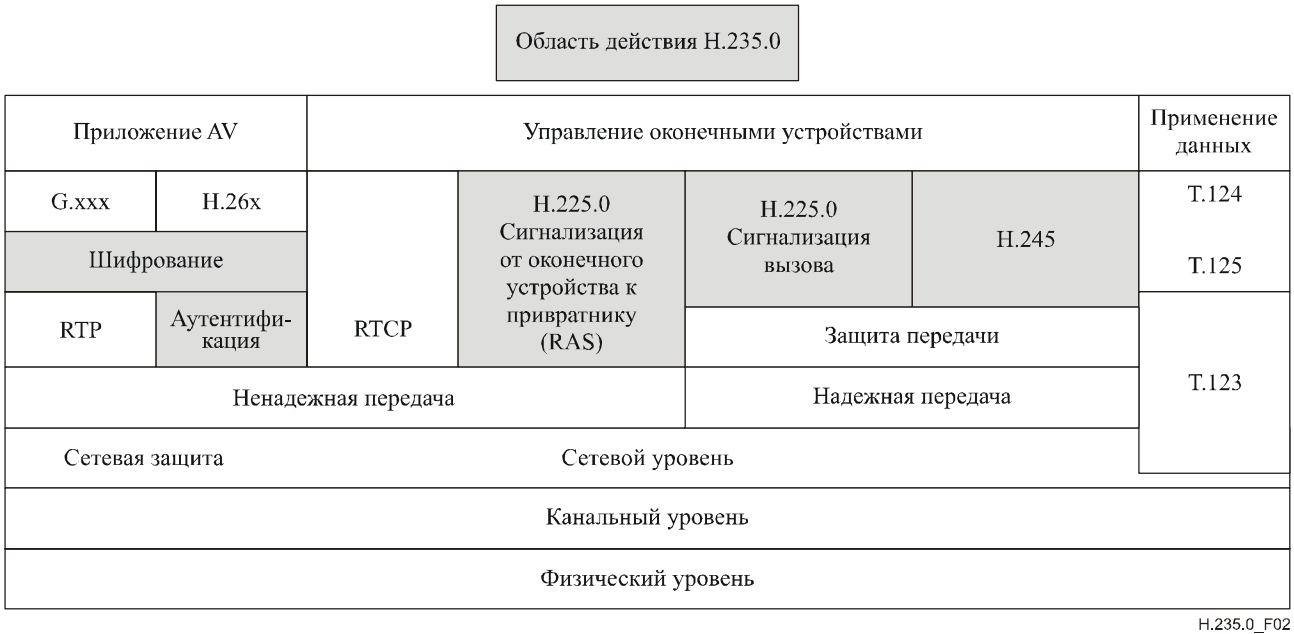
В данной Рекомендации определяются различные идентификаторы объектов (OID) для возможностей защиты сигнализации, процедур или алгоритмов защиты. Эти OID относятся к дереву иерархии присвоенных значений, которые могут возникать из внешних источников или являться частью дерева OID, поддерживаемого МСЭ-Т. Эти OID, которые в особенности относятся к Рек. МСЭ-Т H.235, имеют следующий вид в тексте:

"OID" = {itu-t (0) recommendation (0) h (8) 235 version (0) **V N**}, где **V** представляет собой одиночную десятичную цифру, означающую соответствующую версию Рек. МСЭ-Т H.235; например, 1, 2, 3 или 4. **N** представляет собой десятичное число, однозначно определяющее отдельный экземпляр OID и, следовательно, процедуру, алгоритм или возможность защиты.

Таким образом, закодированный ASN.1 OID состоит из последовательности чисел. Для удобства текстовая мнемоническая условная строчная запись каждого OID используется в тексте как "OID". Дано отображение, которое соотносит каждую строку OID с последовательностью чисел ASN.1. В реализациях, соответствующих Рек. МСЭ-Т H.235, должны использоваться только кодированные ASN.1 числа.

6 Введение в систему

На рисунке 2 дается представление об области применения данной Рекомендации внутри Рек. МСЭ-Т H.323.



H.235.0_F02

Рисунок 2/H.235.0 – Обзор

Для Рек. МСЭ-Т H.323 сигнализация использования TLS (RFC 2246, RFC 3546), IPsec или собственнического механизма канала контроля H.245 должна происходить на защищенном или незащищенном канале H.225.0 в течение начального обмена сообщениями Q.931.

6.1 Резюме

1) Канал сигнализации вызова может быть защищен с использованием TLS (RFC 2246, RFC 3546) или IPsec (RFC 2401, [ESP]) на известном безопасном порту (Рек. МСЭ-Т H.225.0).

2) Пользователи могут быть идентифицированы при начальной установке соединения, в процессе защиты канала H.245 и/или при обмене сертификатами в канале H.245.

3) Возможности шифрования канала медиа определяются расширениями существующего механизма согласования возможностей.

4) Начальное распространение материала ключа от владельца происходит посредством сообщений H.245 **OpenLogicalChannel** или **OpenLogicalChannelAck**.

5) Повторное распространение ключей может совершаться посредством команд H.245: **EncryptionUpdateCommand**, **EncryptionUpdateRequest**, **EncryptionUpdate** и **EncryptionUpdateAck**.

6) Распространение материала ключа защищено либо работой канала H.245 в качестве частного канала, либо специфической защитой материала ключа с использованием выбранных обмениваемых сертификатов.

7) Представленные протоколы защиты соответствуют либо издаваемым стандартам ИСО, либо предлагаемым стандартам IETF.

6.2 Аутентификация

В процессе аутентификации проверяется, являются ли ответчики в действительности теми, за кого себя выдают. Аутентификация может совершаться совместно с обменом сертификатами на основе открытого ключа. Аутентификация может также совершаться посредством обмена, использующего общий секрет между участвующими объектами. Он может быть статическим паролем или какой-либо другой *априорной* информацией.

В данной Рекомендации описывается протокол обмена сертификатами, но не указываются критерии, по которым они совместно проверяются и принимаются. В основном, сертификаты дают некую гарантию проверяющему, что предъявляющий сертификат является тем, за кого себя выдает. Смысл, стоящий за обменом сертификатами, заключается в аутентификации *пользователя* конечной точки, а не просто физической конечной точки. Используя цифровые сертификаты, протокол аутентификации подтверждает, что ответчики владеют частными ключами, соответствующими открытым ключам, содержащимся в сертификате. Эта аутентификация защищает от атак через посредника, но автоматически не доказывает, кем являются ответчики. Нормальное ее выполнение требует наличия неких правил, касающихся остального содержимого сертификатов. Например, если говорить о сертификатах авторизации, сертификат может содержать идентификацию поставщика услуг наряду с формой идентификации учетной записи пользователя, назначенной поставщиком услуг.

В инфраструктуре аутентификации данной Рекомендации не назначается содержимого сертификатов (т. е. не устанавливаются правила, касающиеся сертификатов) свыше того, которое требует протокол аутентификации. Однако приложения, использующие эту инфраструктуру, могут налагать требования политики высокого уровня, таких как предоставление сертификата пользователю для подтверждения. Политика высокого уровня может либо автоматически контролироваться внутри приложения, либо требовать воздействия человека.

Для аутентификации, не использующей цифровые подписи, в данной Рекомендации предусмотрена сигнализация, чтобы осуществить различные сценарии запроса/ответа. Этот метод аутентификации требует предварительной координации связанных объектов, чтобы было возможным получение общего секрета. Примером этого метода может служить клиент обслуживания службы, основанной на подписях.

В третьем варианте аутентификация может совершаться внутри отдельного протокола защиты, такого как TLS (RFC 2246, RFC 3546) или RFC 2409 [IKE].

Равными объектами может поддерживаться и двунаправленная, и однонаправленная аутентификация. Эта аутентификация может проходить на нескольких или на всех каналах связи.

Все специфические механизмы аутентификации, описанные в данной Рекомендации, являются идентичными или взятыми из разработанных ИСО алгоритмов, как указанные в Частях со 2 по 3 в ИСО/МЭК 9798, или основанными на протоколах IETF.

6.2.1 Сертификаты

Стандартизация сертификатов, включая их создание, администрирование и распространение, выходит за рамки области применения данной Рекомендации. Сертификаты, используемые для образования защищенных каналов (сигнализации вызова и/или контроля вызова), должны соответствовать предписанным любым протоколом согласования, чтобы защитить канал.

Следует отметить, что для аутентификации с использованием сертификатов открытого ключа требуется, чтобы конечные точки обеспечили цифровые подписи, используя значения частного ключа. Один только обмен сертификатами открытого ключа не защищает от атак через посредника. Протоколы H.235 соответствуют этому требованию.

6.3 Защита установления вызова

Существуют, по меньшей мере, две причины, по которым требуется обезопасить канал осуществления вызова (например, в H.323 используется Q.931). Первая причина заключается в простой аутентификации перед принятием вызова. Вторая причина: чтобы разрешить авторизацию вызова. Если в оконечном устройстве серии H желательна эта выполняемая функция, то следует использовать безопасный режим связи (как TLS/IPsec для H.323) перед обменом сообщениями установки соединения. В качестве альтернативы авторизация может быть обеспечена на основании аутентификации специфики услуг. Описание принципов авторизации специфики услуг выходит за рамки этой Рекомендации.

6.4 Защита контроля вызова (H.245)

Канал контроля вызова (H.245) также следует защитить каким-либо методом, чтобы обеспечить последующую секретность среды. Канал H.245 должен быть защищен посредством какого-либо согласованного механизма секретности (сюда включен вариант "никакого"). Сообщения H.245 используются, чтобы сигнализировать шифровальные алгоритмы и шифровальные ключи, используемые в совместно используемых частных каналах медиа. Возможность это осуществить в логическом канале базисом логического канала позволяет различным каналам медиа быть зашифрованными посредством различных механизмов. Например, в многоточечных централизованных конференциях могут быть использованы различные ключи к потокам к каждой конечной точке. Это позволяет потокам медиа быть частными для каждой конечной точки конференции. Для того чтобы использовать сообщения H.245 защитным методом, весь канал H.245 (логический канал 0) следует открыть согласованным защитным методом.

Механизм, посредством которого H.245 делается защищенным, зависит от участвующих оконечных устройств серии H. Единственное требование от всех систем, использующих эту структуру защиты, заключается в том, что каждая должна иметь некий метод, которым она согласуется и/или сигнализирует, что с каналом H.245 нужно работать в особой защищенной манере, перед тем как он будет действительно инициирован. Например, чтобы достичь этого, H.323 будет использовать сообщения сигнализации соединения H.225.0.

6.5 Секретность потока медиа

В данной Рекомендации описана секретность среды для потоков медиа, переносимых в пакетных сетях передачи. Эти каналы могут быть однонаправленными в отношении характеристик логического канала H.245. От каналов не требуется быть однонаправленными на физическом или транспортном уровне.

Первым шагом в достижении секретности среды должно являться обеспечение частным каналом контроля, в котором устанавливается криптографический ключевой материал и/или устанавливаются

логические каналы, которые будут переносить потоки шифрованной информации. Для этой цели при работе в защищенной конференции, любые участвующие конечные пункты могут использовать зашифрованный канал H.245. В этом методе выбор криптографического алгоритма и ключи шифрования, как принято в команде **OpenLogicalChannel** H.245, защищены.

С защищенным каналом H.245 можно работать, используя характеристики, отличные от характеристик в частном канале (каналах) медиа, пока это обеспечивает совместно приемлемый уровень секретности. Это позволяет механизмам защиты, защищающим потоки медиа и любые каналы контроля, функционировать совершенно независимым образом, обеспечивая полностью различные по силе и сложности уровни.

Требуется, чтобы с каналом H.245 работали методом без шифрования, специфические шифровальные ключи медиа могут быть шифрованы раздельно методом, сигнализированным и установленным группами-участниками. Логический канал типа **h235Control** можно использовать, чтобы обеспечить материал для защиты шифровальных ключей медиа. С логическим каналом можно работать в любом подходяще согласованном режиме.

Секретность (шифрование) данных, переносимых по логическим каналам, должна быть представлена в форме, определяемой **OpenLogicalChannel**. Заголовочная информация специфики передачи не должна шифроваться. Секретность данных должна основываться на комплексном шифровании.

6.6 Защитные элементы

Основу для аутентификации (доверия) и секретности определяют оконечные устройства канала связи. Для канала установления соединения они могут находиться между осуществляющим вызов и хостинговым сетевым компонентом. К примеру, телефон "доверяет" тому, что коммутатор соединит его с телефоном, номер которого был набран. По этой причине любой объект, оканчивающий канал контроля H.245 или логический канал любого типа **encryptedData**, должен рассматриваться как доверенный элемент соединения; они могут включать MC(U) и шлюзы. Результатом доверия элементу является доверенность в раскрытии механизма секретности (алгоритма и ключа) этому элементу.

В добавление к вышесказанному, аутентификация отдельных и всех "доверенных" элементов возлагается на участников, стоящих на пути связи. Это будет нормально выполнено посредством обмена сертификатами, как происходит для "стандартной" аутентификации из конца в конец. В данной Рекомендация не будет требоваться специфического уровня аутентификации, а лишь будет предложено, чтобы он был приемлем для всех объектов, использующих доверенный элемент. Подробности о доверительной модели и правилах, касающиеся сертификатов, будут исследованы далее.

Между двумя точками может быть гарантирована секретность, только если подтверждено, что связи между доверенными элементами защищены от атак через посредника.

6.6.1 Условное депонирование ключа

Хотя для работы это и не особенно требуется, данная Рекомендация содержит условие поддержки объектами, использующими протокол H.235, услуги, известной как третья доверенная группа (TTP) внутри элементов сигнализации.

Возможность восстановления потерянных шифровальных ключей медиа следует поддерживать в установках, где эта выполняемая функция желательна или требуема.

Условное депонирование ключа – это услуга, к которой часто обращаются, как к третьей доверенной группе (TTP). Эта услуга будет исследована далее.

6.7 Невозможность отказа

Для дальнейшего исследования.

6.8 Конфиденциальность подвижной связи

Системы, основанные на H.323, могут использоваться в среде подвижной связи, согласно Рек. МСЭ-Т H.510. Процедуры и протоколы защиты для таких систем описаны в Рек. МСЭ-Т H.530. В Рек. МСЭ-Т H.530 используются протоколы и процедуры из данной Рекомендации.

6.9 Профили защиты

В данной Рекомендации есть ссылки на пару профилей защиты H.235 (т. е. H.235.1, H.235.2, H.235.3, H.235.4, H.235.5, H.235.6, H.235.7, H.235.8 и H.235.9). В профиле защиты указано использование специфики H.235 или подмножества выполняемых функций H.235 для хорошо определенных сред с обозначенным применением.

В зависимости от среды и приложения, профили защиты могут быть использованы выборочно или все вместе. Характерно, что системы, введенные H.235, указывают на внутренние идентификаторы объектов как на часть сигнальных сообщений, чьи профили защиты они используют. Системам, введенным H.235, профиль защиты следует выбирать в соответствии с их потребностями.

К тому же, конечные точки могут предлагать несколько профилей защиты одновременно в сообщениях **RRQ**/**GRQ** и позволять привратнику выбирать наиболее пригодный, давая ответ сообщением **RCF**/**GCF**. Транзакции **LRQ**/**LCF** между привратниками также могут нести несколько профилей защиты. При вычислении цифровых подписей или значений хэша для обеспечения целостности сообщения сначала следует вычислить значения хэша и цифровых подписей, не обеспечивающих целостность сообщения, через подмножество и множество поля в сообщении, все значения цифровых подписей и хэша, обеспечивающих целостность сообщения, следует установить в ноль в буфере сообщения, затем все значения цифровых подписей и хэша следует вычислить с использованием этого буфера и затем записать в сообщение.

Каждая из подсерий Рекомендаций написана как профиль защиты H.235.0. Профиль защиты H.235.0 характерно включает специфический случай использования H.235.0 внутри отдельного сценария и/или содержит отдельную спецификацию защиты или комбинацию механизмов защиты/профилей защиты.

Все профили защиты являются дополнительными внутри H.235.0.

На рисунке 3 иллюстрированы некоторые типичные и возможные комбинации профилей защиты. Сплошной линией показано, что парная комбинация профилей защиты определена и возможна. Пунктирной линией показано, что комбинация вообще возможна, но комбинация может быть не очень полезна. Отсутствие линий означает, что такая комбинация пока еще не определена.

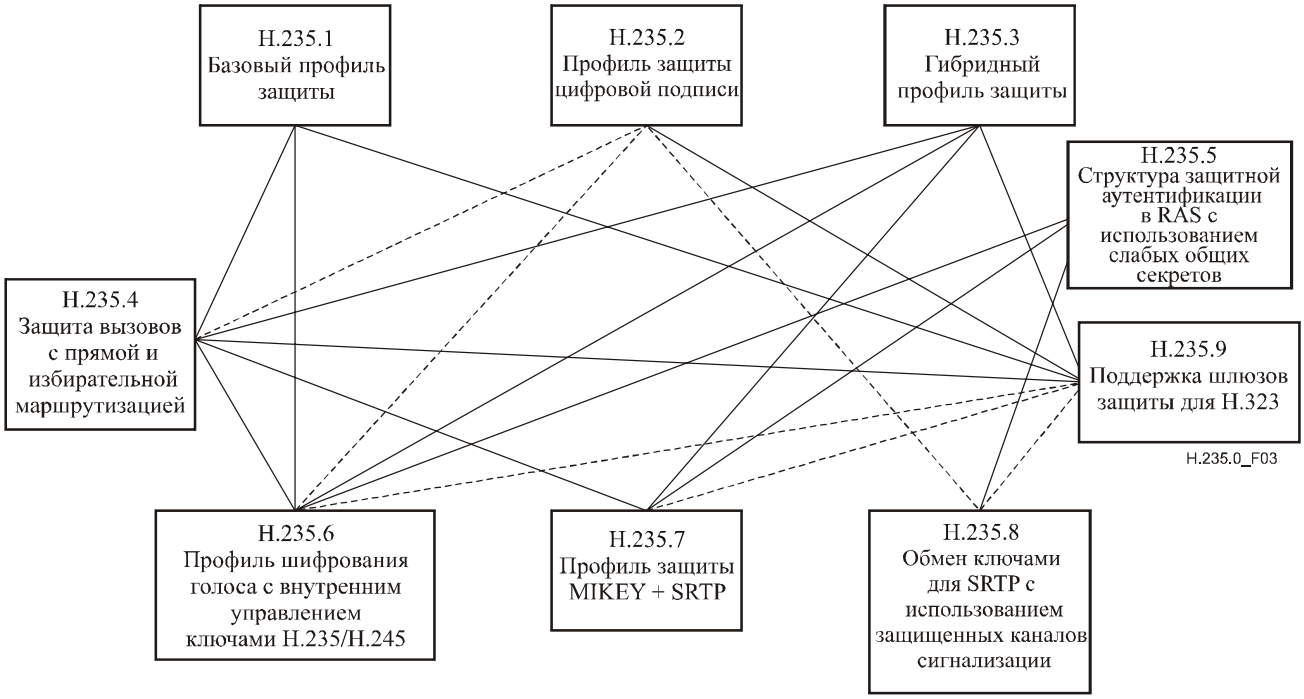


Рисунок 3/H.235.0 – Иллюстрация комбинаций профилей защиты

6.10 Прохождение через защищенные NAT/сетевые экраны

В Рек. МСЭ-Т H.235.9 изложены процедуры обнаружения шлюзов защиты (как ALG) на пути сигнализации H.225.0 RAS между объектами H.323 (привратник, конечная точка) и того, как привратник и шлюз защиты совместно используют информацию о защите, чтобы сохранить целостность и секретность сигнализации.

В Рекомендациях МСЭ-Т H.235.1 (метод IA) и H.235.2 (метод только аутентификации) предлагаются дополнительные особые процедуры, позволяющие основанной на H.235 аутентификации сообщений RAS H.225.0 и протоколам сигнализации вызова проходить через устройства NAT/сетевые экраны.

7 Процедуры осуществления соединения

Как было изложено в пункте "Введение в систему", и канал установки соединения (H.225.0 для серии H.323), и канал контроля вызова (H.245) должны функционировать в согласованном защищенном или незащищенном режиме, начиная с первого обмена. Для канала установки соединения это делается *априорно* (для H.323 защищенная TLS TSAP (порт 1300) должна использоваться для сообщений Q.931). Для канала контроля вызова режим защиты определяется информацией, проходящей по протоколу начального установления соединения, используясь оконечным устройством серии H.

В случаях когда нет совпадающих возможностей защиты, вызываемое оконечное устройство может отклонить соединение. Возвращаемая ошибка не должна нести информацию о несоответствиях в защите; вызывающее оконечное устройство должно определить эту проблему какими-нибудь другими способами. В случаях когда вызывающее оконечное устройство получает сообщение без обоснования возможностей защиты, оно должно прервать вызов.

Если вызывающее и вызываемое оконечные устройства имеют совместимые возможности защиты, обеими сторонами должно быть допущено, что канал H.245 должен функционировать в согласованном защищенном режиме. Невозможность установления канала H.245 в определенный защищенный режим здесь следует рассматривать как ошибку протокола, и соединение следует прервать.

Рек. МСЭ-Т H.235.6 предусматривает дальнейшие процедуры защиты установления соединения, включая управление ключом; см. пп. 7 и 8/H.235.6.

8 Сигнализация и процедуры аутентификации

Аутентификация, в основном, основывается либо на использовании общего секрета (вас должным образом аутентифицируют, если вы знаете секрет), либо на методах открытого ключа с сертификатами (вы доказываете свою подлинность, предоставляя правильный частный ключ). Общий секрет и последующее использование симметричного шифрования требуют предварительного соединения между взаимодействующими объектами. Предварительную диалоговую или защищенную связь можно заменить генерацией или обменом общим секретным ключом методами, основанными на шифровании открытым ключом, например, обменом ключами Диффи-Хеллмана. Группы, участвующие в обмене информацией, при генерации и обмене ключами, должны быть аутентифицированы, например, сообщениями с цифровыми подписями; иначе участвующие в обмене информацией группы не могут быть уверены в том, с кем они совместно используют секрет.

В этой Рекомендации представлены методы аутентификации, основанные на абонировании, т. е. должно произойти предварительное соединение для совместного использования секрета, и методы аутентификации, где шифрование открытым ключом напрямую используется для аутентификации или используется для генерации общего секрета.

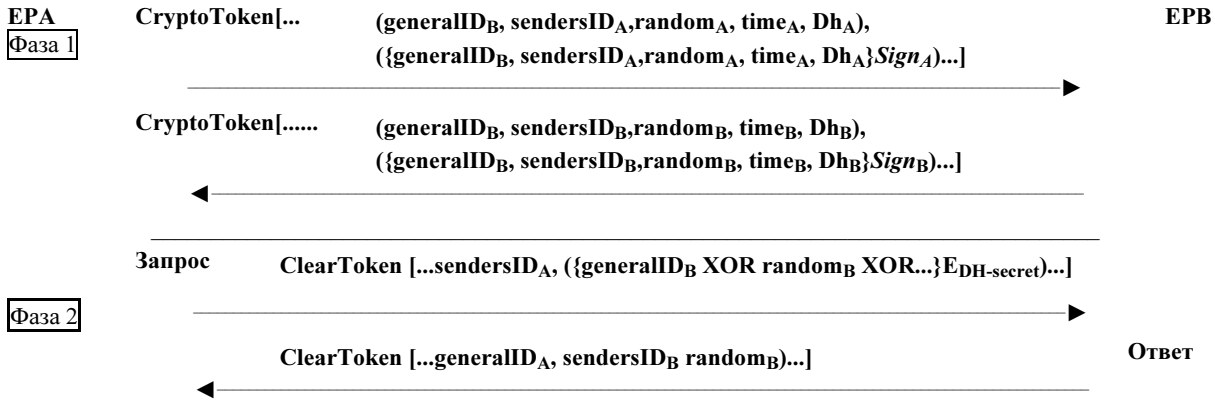
8.1 Схема Диффи-Хеллмана с дополнительной аутентификацией

Смысл заключается в том, чтобы не обеспечивать абсолютной аутентификации на пользовательском уровне. Этот метод предусматривает сигнализацию, чтобы сгенерировать общий секрет между двумя объектами, который может обеспечить материал шифрования для частной связи.

В конце этого обмена оба объекта будут обладать общим секретным ключом вместе с выбранным алгоритмом, посредством которого используется этот ключ. Теперь этот общий секретный ключ может быть использован в любых дальнейших обменах запроса/ответа. Следует заметить, что в редких случаях обмен по Диффи-Хеллману может генерировать так называемые *слабые* ключи для особых алгоритмов. В этом случае каждый объект должен отсоединиться и подсоединиться вновь для образования нового набора ключей.

В первой фазе рисунка 4 демонстрируются данные, обмениваемые в течение процесса Диффи-Хеллмана. Во второй фазе сообщениям запроса приложения или специфики протокола позволяется быть аутентифицированными ответчиком. Обратите внимание, что с каждым ответом может возвращаться новое случайное значение.

ПРИМЕЧАНИЕ. – Если обмен сообщениями происходит на незащищенном канале, то нужно использовать цифровые подписи (или другие сообщения, составляющие метод аутентификации), чтобы аутентифицировать группы, которыми будет совместно использоваться секрет. Также могут быть предусмотрены дополнительные элементы подписей; они иллюстрированы ниже ***курсивом***.



[.....] обозначает последовательность маркеров.

() обозначает отдельный маркер, который может содержать несколько элементов.

{}E$_{DH\text{-}secret}$ обозначает содержащиеся значения, зашифрованные с использованием секрета Диффи-Хеллмана.

EPB знает, какой общий секретный ключ использовать, чтобы дешифровать идентификатор **generalID$_B$**, соотнося его с **generalID$_A$**, который также должен проходить в сообщении как **sendersID$_A$**. Заметьте, что зашифрованное значение в Фазе 2 проходит в поле **generalID clearToken** для упрощения шифрования.

Рисунок 4/H.235.0 – схема Диффи-Хеллмана с дополнительной идентификацией

8.2 Аутентификация на основе подписей

Несмотря на то, что процедуры, отмеченные здесь (и алгоритмы ИСО, из которых они получены), по природе своей двунаправленные, они могут быть использованы только в одном направлении, если аутентификация необходима только в этом направлении. Описаны как двухпроходные, так и трехпроходные процедуры. Взаимная двухпроходная аутентификация может быть выполнена только в одном направлении, когда сообщения, возникающие в обратном направлении, не нужно аутентифицировать. Эти обмены допускают, что каждая сторона обладает каким-то хорошо известным идентификатором (таким как текстовый идентификатор), который уникальным образом идентифицирует ее. Для двухпроходной процедуры делается дальнейшее допущение, что есть взаимно приемлемая отсылка на время (от которого отмеряются временные отметки). Приемлемое временное отклонение является предметом локальной реализации. Трехпроходные процедуры используют случайно генерируемое, непредсказуемое запрашиваемое число (которое может быть увеличено последовательным счетчиком 'random') как запрос устройства аутентификации. Это случайное число предназначено для защиты от атак взлома защиты путем замещения оригинала (атаки воспроизведения). В отличие от трехпроходных, двухпроходные процедуры не аутентифицируют первоначальное сообщение, удерживая запрос инициатора.

Есть три возможных варианта, которые могут быть использованы в зависимости от требований:

1) на основе пароля с симметричным шифрованием;

2) на основе пароля с хэшированием;

3) на основе сертификатов с подписями.

Во всех случаях маркер будет содержать информацию, как описанная в следующих пунктах, в зависимости от выбранного варианта. Отметим, что во всех случаях **generalID** можно скорее узнать из конфигурации или поиска по справочнику, чем в протокольном обмене полосы. Чтобы упростить обработку на приемнике, отправитель должен включить свою подлинность в **sendersID** и установить **generalID** на идентификацию получателя.

ПРИМЕЧАНИЕ 1. – Во всех случаях, где временные отметки генерируются и проходят как часть обмена защиты, осуществляющие должны принять следующие меры предосторожности. Зернистость временных отметок должна быть достаточно мелкой, чтобы гарантировалось ее увеличение с каждым сообщением. Если оно не гарантируется, возможны атаки воспроизведения. (Например, если временная отметка возрастает только на минуту, то конечная точка "C" может обманывать "A" в пределах длительности одной минуты после того, как конечная точка "A" послала сообщение конечной точке "B").

ПРИМЕЧАНИЕ 2. – Если сообщение многоадресное, то оно не защищено.

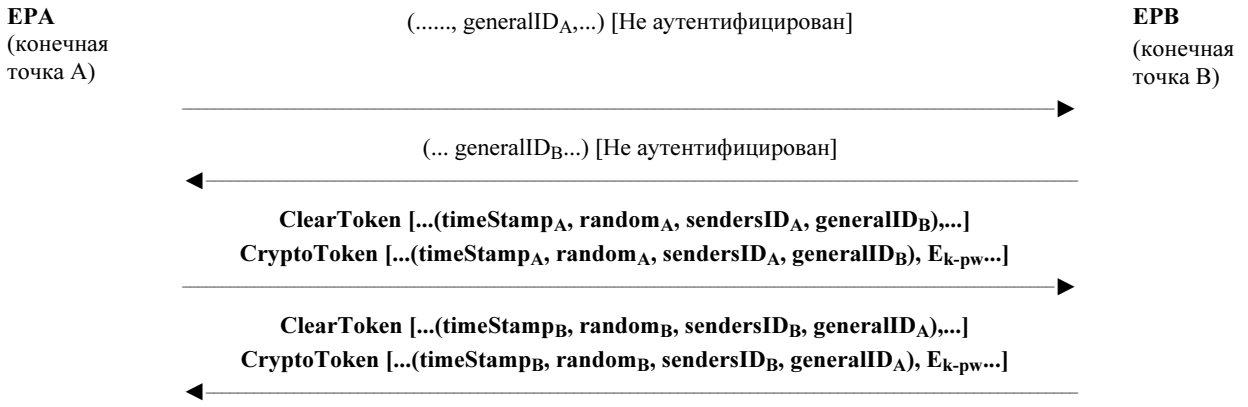
8.2.1 Пароль с симметричным шифрованием

На рисунках 5 и 6 показаны формат маркера и обмен сообщениями, требуемые для выполнения этого типа аутентификации в два прохода или в три прохода, соответственно. Этот протокол основан на пунктах 5.2.1 (двухпроходный) и 5.2.2 (трехпроходный) ИСО/МЭК 9798-2; допускается, чтобы идентификатором и относящимся к нему паролем обменивались в процессе шифрования. Длина шифровального ключа N октетов (как указано в AlgorithmID), и он формируется следующим образом:

– Если длина пароля = N, Ключ = паролю;

– если длина пароля < N, ключ заполнен нулями;

– если длина пароля > N, первые N октетов присваиваются ключу, затем N + M-й октет пароля преобразуется посредством XOR в Mmod(N)-*й* октет (для всех октетов после N) (т. е. все "дополнительные" октеты пароля повторно откатываются назад по ключу посредством XOR).



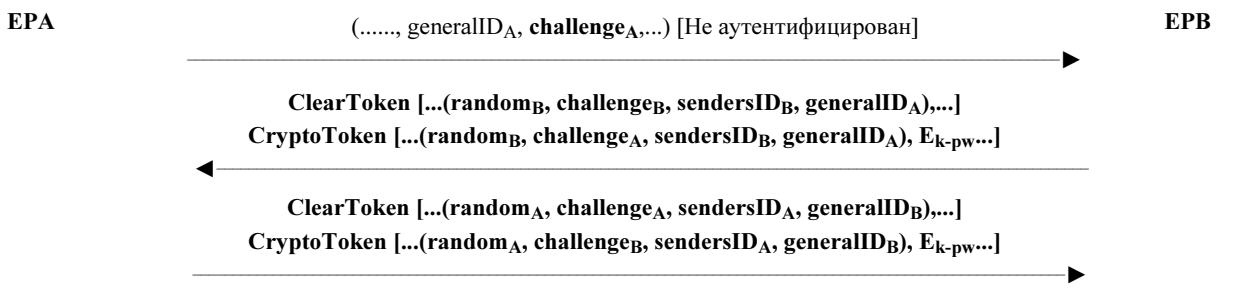
ПРИМЕЧАНИЕ 1. – Маркер, возвращаемый из EPB, дополнительный; если он отсутствует, достигается только однонаправленная аутентификация.

ПРИМЕЧАНИЕ 2. – $\mathbf{E_{k-pw}}$ показывает значения, зашифрованные с использованием ключа "k", полученного из пароля "pw".

ПРИМЕЧАНИЕ 3. – **random** – монотонно возрастающий счетчик, делающий несколько сообщений с одной временной отметкой уникальными.

ПРИМЕЧАНИЕ 4. – В третьем сообщении EPA обеспечивает отдельный **ClearToken**, который идентифицируется таким же OID, как OID в **CryptoToken**; так же и в четвертом сообщении, и наоборот.

Рисунок 5/H.235.0 – Пароль с симметричным шифрованием; два прохода



ПРИМЕЧАНИЕ 1. – **challenge$_A$** и его возврат, зашифрованные **CryptoToken** из B в A, не нужны, если желательна однонаправленная аутентификация.

ПРИМЕЧАНИЕ 2. – $\mathbf{E_{k-pw}}$ обозначает шифровальную функцию, шифруемую с использованием ключа "k", полученного из пароля "pw".

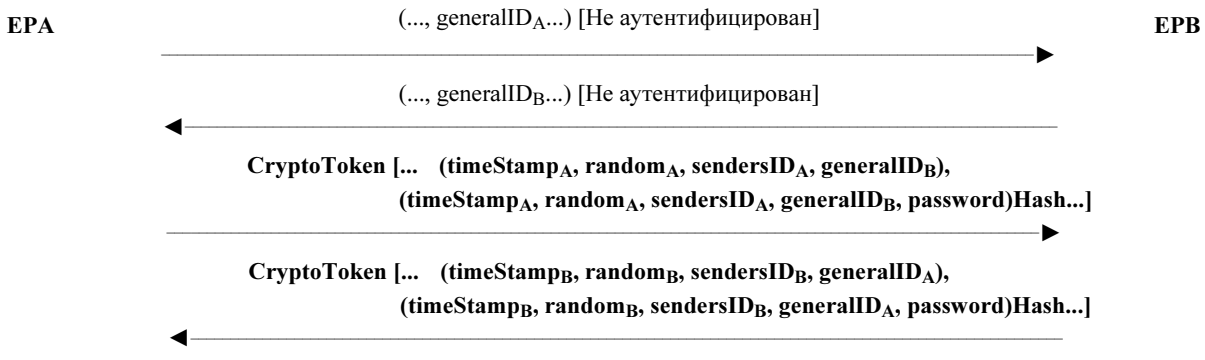
ПРИМЕЧАНИЕ 3. – В третьем сообщении EPA обеспечивает новый **challenge$_A$** открытым текстом в отдельном **ClearToken**, который идентифицируется таким же OID, как OID в **CryptoToken**. EPA также возвращает зашифрованный **challenge$_B$** в качестве ответа; так же и во втором сообщении, и наоборот.

ПРИМЕЧАНИЕ 4. – Из множества видных сообщений **random** (т. е. монотонно возрастающий счетчик) должен сделать запрос уникальным.

Рисунок 6/H.235.0 – Пароль с симметричным шифрованием; три прохода

8.2.2 Пароль с хэшированием

Рисунки 7 и 8 показывают формат маркера и обмен сообщениями, требуемые для выполнения этого типа аутентификации в два прохода или в три прохода, соответственно. Этот протокол основан на пунктах 5.2.1 и 5.2.2 ИСО/МЭК 9798-4; допускается, чтобы идентификатором и относящимся к нему паролем обменивались в процессе шифрования. В Рек. МСЭ-Т H.235.1 предусмотрено подробное описание двухпроходной процедуры хэширования.

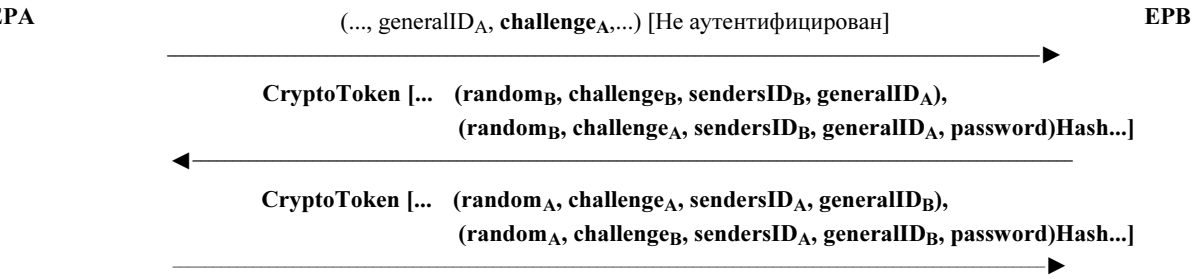


ПРИМЕЧАНИЕ 1. – Маркер, возвращаемый из EPB, дополнительный; если он отсутствует, достигается только однонаправленная аутентификация.

ПРИМЕЧАНИЕ 2. – **Hash** обозначает хэш-функцию, которая работает с содержащимися значениями.

ПРИМЕЧАНИЕ 3. – **random** – монотонно возрастающий счетчик, делающий несколько сообщений с одной временной отметкой уникальными.

Рисунок 7/H.235.0 – Пароль с хэшированием; два прохода



ПРИМЕЧАНИЕ 1. – Маркер, возвращаемый из EPB, дополнительный; если он отсутствует, достигается только однонаправленная аутентификация.

ПРИМЕЧАНИЕ 2. – **Hash** обозначает хэш-функцию, которая работает с содержащимися значениями.

ПРИМЕЧАНИЕ 3. – В третьем сообщении EPA обеспечивает новый **challenge$_A$** открытым текстом со встроенным **ClearToken** в **cryptoHashedToken**. EPA также возвращает хэшированный **challenge$_B$** в качестве ответа; так же и для второго сообщения, и наоборот

ПРИМЕЧАНИЕ 4. – Из множества видных сообщений **random** (т. е. монотонно возрастающий счетчик) должен сделать запрос уникальным.

Рисунок 8/H.235.0 – Пароль с хэшированием; три прохода

ПРИМЕЧАНИЕ 1. – Структура **cryptoHashedToken** используется для передачи параметров, используемых в этом сообщении. Будучи включены в эту структуру, есть 'чистые' версии параметров, необходимые для вычисления хэшированного значения. Осуществляющие должны включить временную отметку в **hashedVals** и *не* должны включать пароль. (Например, и пароль, и '**generalID**' должны быть *априорно* известны получателю; первый может отсутствовать)

ПРИМЕЧАНИЕ 2. – Хэш-функция должна быть применима к структуре **EncodedGeneralToken**, включающей, по меньшей мере, поля ID, временной отметки и пароля. Значение пароля НЕ должно передаваться в **ClearToken**.

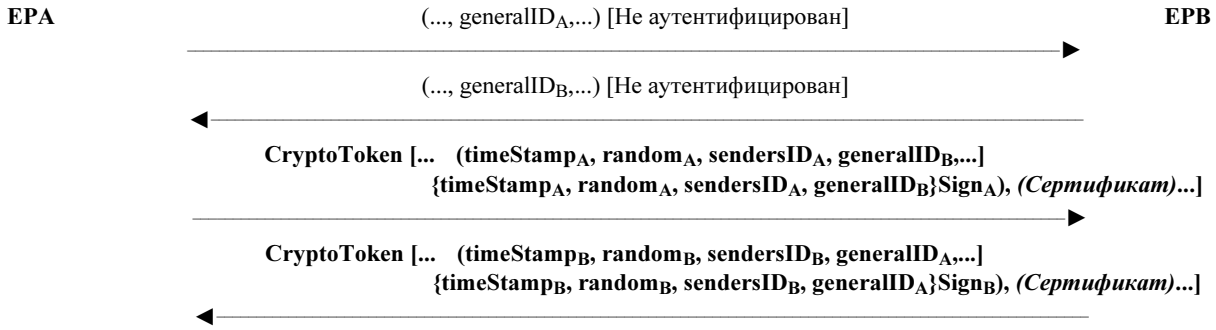
ПРИМЕЧАНИЕ 3. – Осуществляющие должны убедиться, что вводимые пользователем пароли несут в себе достаточную энтропию. Слишком короткие пароли, которые чувствительны к подборам по словарю, должны быть отклонены. Проведение введенной пользователем фразы пароля через криптографическую хэш-функцию и использование битов, полученных на выходе, в определенных случаях может оказаться весьма полезным.

8.2.3 Вариант, основанный на сертификатах с подписями

На рисунках 9 и 10 показаны формат маркера и обмен сообщениями, требуемые для выполнения этого типа аутентификации. Этот протокол основан на пункте 5.2.1 ИСО/МЭК 9798-3; допускается, чтобы идентификатором и относящимся к нему сертификатом обменивались в процессе шифрования. В Рек. МСЭ-Т H.235.2 предусмотрено подробное описание двухпроходной процедуры с использованием подписей.

ПРИМЕЧАНИЕ 1. – Также может быть предусмотрен дополнительный элемент сертификата; они иллюстрированы ***курсивом*** внизу.

ПРИМЕЧАНИЕ 2. – Если сообщение многоадресное, то идентификатор места назначения (**generalID$_B$** для сообщений, происходящих из A и наоборот) не должен быть включен в **ClearToken**.



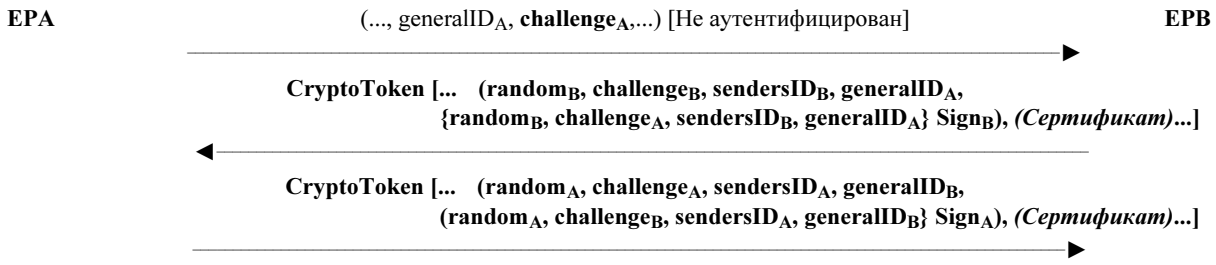
ПРИМЕЧАНИЕ 1. – Маркер, возвращаемый из EPB, дополнительный; если он отсутствует, достигается только однонаправленная аутентификация.

ПРИМЕЧАНИЕ 2. – Сертификат типа "оплата" может дополнительно быть включен в источник EPA.

ПРИМЕЧАНИЕ 3. – **Sign** обозначает подписывающую функцию (из соответствующего сертификата), выполняемую по содержащимся значениям.

ПРИМЕЧАНИЕ 4. – **random** – монотонно возрастающий счетчик, делающий несколько сообщений с одной временной отметкой уникальными.

Рисунок 9/H.235.0 – Вариант, основанный на сертификатах с подписями; два прохода



ПРИМЕЧАНИЕ 1. – Маркер, возвращаемый из EPB, дополнительный; если он отсутствует, достигается только однонаправленная аутентификация.

ПРИМЕЧАНИЕ 2. – Сертификат типа "оплата" может дополнительно быть включен в источник EPA.

ПРИМЕЧАНИЕ 3. – **Sign** обозначает подписывающую функцию (из соответствующего сертификата), выполняемую по содержащимся значениям.

ПРИМЕЧАНИЕ 4. – В третьем сообщении EPA обеспечивает новый **challenge$_A$** открытым текстом внутри встроенного шифрованного **GeneralToken**. EPA также возвращает подписанное **challenge$_B$** в качестве ответа; так же и для второго сообщения, и наоборот.

ПРИМЕЧАНИЕ 5. – Из множества видных сообщений **random** (т. е. монотонно возрастающий счетчик) должен сделать вызов уникальным.

Рисунок 10/H.235.0 – Вариант, основанный на сертификатах с подписями; три прохода

8.2.4 Использование общего секрета и паролей

В данной Рекомендации применяются определенные методы симметричного шифрования для целей аутентификации, целостности и конфиденциальности. Когда употребляются симметричные методы, в этом тексте используются термины пароль и общий секрет 21. Общий секрет понимается как характерный термин, определяющий произвольную битовую строку. Общий секрет может быть

назначен или скомпонован как часть процесса подписания пользователем или быть частью внутриканального вычисления, как полученный по Диффи-Хеллману общий секрет.

Пароль можно рассматривать как буквенно-цифровую строку, которую пользователи могут запомнить. Очевидно, что использование паролей должно проходить с особой аккуратностью. Пароли способны обеспечить достаточную безопасность, только когда они выбираются случайно из большого пространства, когда они несут достаточную энтропию, такую, что они непредсказуемы, и когда их периодически меняют. Правила, касающиеся установления и хранения паролей, выходят за рамки области применения данной Рекомендации.

Хорошей практикой получения выгоды от использования паролей может являться преобразование строки пароля пользователя в фиксированную битовую строку, как общий секрет с использованием криптографически сильной односторонней хэш-функции.

В качестве рекомендуемого примера, при использовании профиля защиты H.235.1 SHA1 при применении к строке пароля дает 20-байтовый общий секрет. Преимущество заключается в том, что результат хэширования не только скрывает настоящий пароль, но и определяет формат битовой строки фиксированной длины, не жертвуя для этого энтропией.

Так,

общий секрет := SHA1 (пароль)

8.3 Сигнализация/процедуры RAS для аутентификации

В данной Рекомендации не предусмотрено подробное описание какой-либо формы секретности сообщений между привратниками и конечными точками. Существуют два типа аутентификации, которые можно использовать. Первый тип основан на симметричном шифровании, он не требует предварительного соединения между конечной точкой и привратником. Второй тип основан на подписях и будет иметь две формы: пароля и сертификата. Все эти формы получаются из процедур, описанных в пунктах 8, 8.2.1, 8.2.2 и 8.2.3. В данной Рекомендации характерные обозначения (EPA и EPB), показанные в вышеназванных пунктах, будут представлять конечную точку и привратника, соответственно.

8.3.1 Аутентификация конечная точка-привратник (не основанная на подписи)

В этом механизме привратник может быть обеспечен криптографической связью. В криптографической связи утверждается о том, что определенная конечная точка, которая была предварительно зарегистрирована, является той же самой, которая высылает последующие сообщения RAS. Следует заметить, что она может не предусматривать какую-либо аутентификацию привратника в конечной точке, кроме включенного дополнительного элемента подписи. Возникновение отношений идентификации происходит, когда оконечное устройство выпускает **GRQ**, как отмечено в 7.2.1/H.323. Обмен по Диффи-Хеллману должен возникать совместно с сообщениями **GRQ** и **GCF**, как показано в первой фазе пункта 8. Этот общий секретный ключ теперь нужно использовать в любых последующих **RRQ**/**URQ** от оконечного устройства к привратнику. Если привратник работает в этом режиме и получает **GRQ** без маркера, содержащего *DHset,* или приемлемого значения алгоритма, он возвратит код обоснования **securityDenial** или другой подходящий код ошибки, согласно 11.1 в **DRJ**.

Общий секретный ключ Диффи-Хеллмана, как созданный при обмене **GRQ**/**GCF**, может быть использован для аутентификации последующих сообщений **xRQ**. Для совершения этого способа аутентификации должны быть использованы следующие процедуры.

Оконечное устройство **(xRQ)**

1) Оконечное устройство должно обеспечить всю информацию в сообщении, как описано в соответствующих пунктах Рек. МСЭ-Т H.225.0.

2) Оконечное устройство должно шифровать **GatekeeperIdentifier** (как возвращаемый в **GCF**), используя общий секретный ключ, который был согласован. Он будет проходить в **clearToken** (см. 8.1) как **generalID**.

16 битов **random**, а затем **requestSeqNum** должны подвергнуться операции XOR с каждыми 16 битами **GatekeeperIdentifier**. Если **GatekeeperIdentifier** не заканчивается даже на границе 16,

последние 8 битов **GatekeeperIdentifier** должны подвергнуться операции XOR с последним значимым октетом случайного значения и затем с **requestSeqNum**. **GatekeeperIdentifier** должен быть зашифрован с использованием выбранного алгоритма в **GCF** (algorithmOID) и с использованием всего общего секрета.

Следующий пример иллюстрирует эту процедуру:

RND16: 16-битовое случайное значение

SQN16: 16-битовое значение requestSeqNum

BMPX: X-й BMP символ GatekeeperIdentifier

BMP1' = (BMP1) XOR (RND16) XOR (SQN16)

BMP2' = (BMP2) XOR (RND16) XOR (SQN16)

BMP3' = (BMP3) XOR (RND16) XOR (SQN16)

BMP4' = (BMP4) XOR (RND16) XOR (SQN16)

BMP5' = (BMP5) XOR (RND16) XOR (SQN16)

:

:

BMPn' = (BMPn) XOR (RND16) XOR (SQN16)

Для того чтобы криптографически связать это и последующие сообщения с первоначально подавшим запрос (конечная точка, выславшая **RRQ**), должно быть использовано чаще всего возвращаемое значение **random** (этим значением может быть то, которое новее, чем значение, возвращаемое в **RCF** из последнего сообщения **xCF**).

Привратник **(xCF/xRJ)**

1) Привратник должен шифровать свой **GatekeeperIdentifier** (следуя вышеописанной процедуре) общим секретным ключом, связанным с псевдонимом конечной точки, и сравнивать это значение со значением в **xRQ**.

2) Привратник должен возвращать **xRJ**, если два зашифрованных значения не совпадают.

3) Если **GatekeeperIdentifier** совпадает, привратник должен принять локальное решение и ответить с помощью **xCF** или **xRJ**.

4) Если привратником посылается **xCF**, оно должно содержать назначенный **EndpointIdentifier** и новое случайное значение в поле **random clearToken**.

Для графического представления этого обмена обращайтесь ко второй фазе рисунка 4. Привратник знает, какой общий секретный ключ использовать, чтобы расшифровать идентификатор привратника по псевдониму в сообщении.

8.3.2 Аутентификация конечная точка-привратник (основанная на подписи)

Все другие, помимо **GRQ**/**GCF**, сообщения RAS должны содержать маркеры аутентификации, требуемые специфическим режимом функционирования. Есть три возможных варианта, которые можно использовать в зависимости от требований и среды:

1) на основе пароля с симметричным шифрованием;

2) на основе пароля с хэшированием;

3) на основе сертификатов с подписями.

Во всех случаях в маркере будет содержаться информация, как описанная в следующих пунктах, в зависимости от выбранного варианта. Если привратник работает в безопасном режиме и получает сообщение RAS без приемлемого значения маркера, он должен возвратить код обоснования **securityDenial** или другой подходящий код ошибки, согласно 11.1 в сообщении отказа. Во всех случаях маркер, возвращаемый от привратника, – дополнительный; если его нет, достигается только однонаправленная аутентификация.

8.3.2.1 Пароль с симметричным шифрованием

Фаза обнаружения привратника (**GRQ**, **GCF** и **GRJ**) может быть незащищена, как показано на рисунке 11, или может быть защищена с использованием **cryptoTokens**.

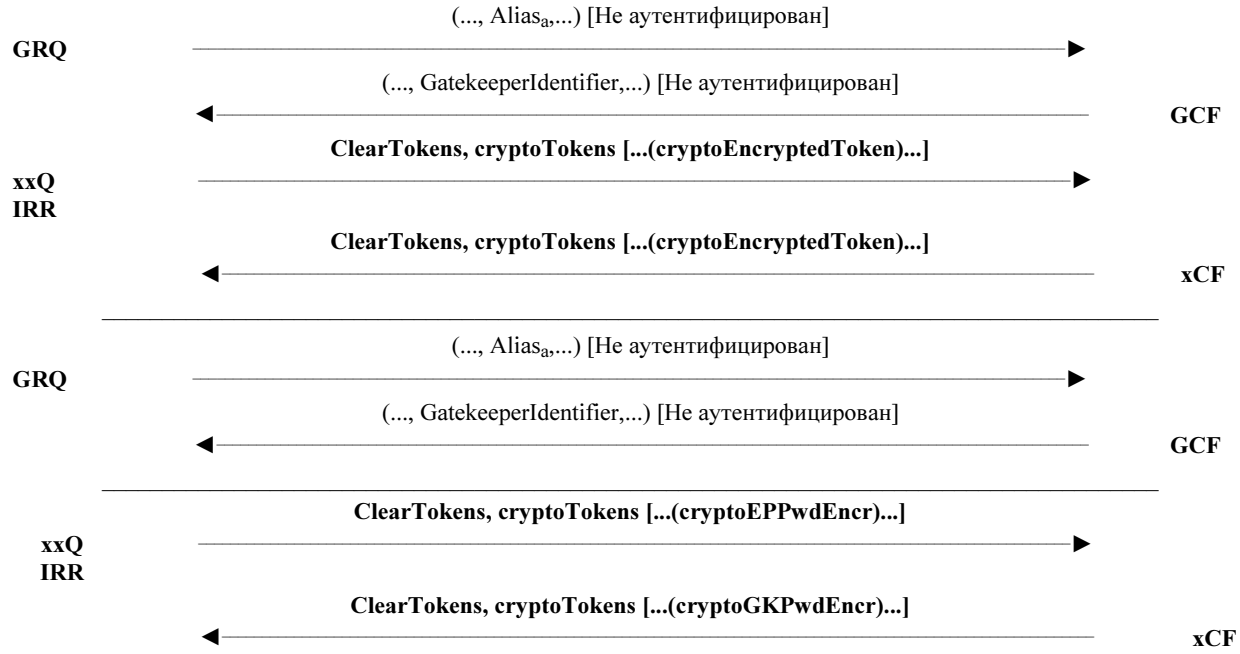


Рисунок 11/H.235.0 – Пароль с симметричным шифрованием

8.3.2.2 Пароль с хэшированием

Фаза обнаружения привратника (**GRQ**, **GCF** и **GRJ**) может быть незащищена, как показано на рисунке 12, или может быть защищена, согласно Рек. МСЭ-Т H.235.1, с использованием **cryptoTokens**.

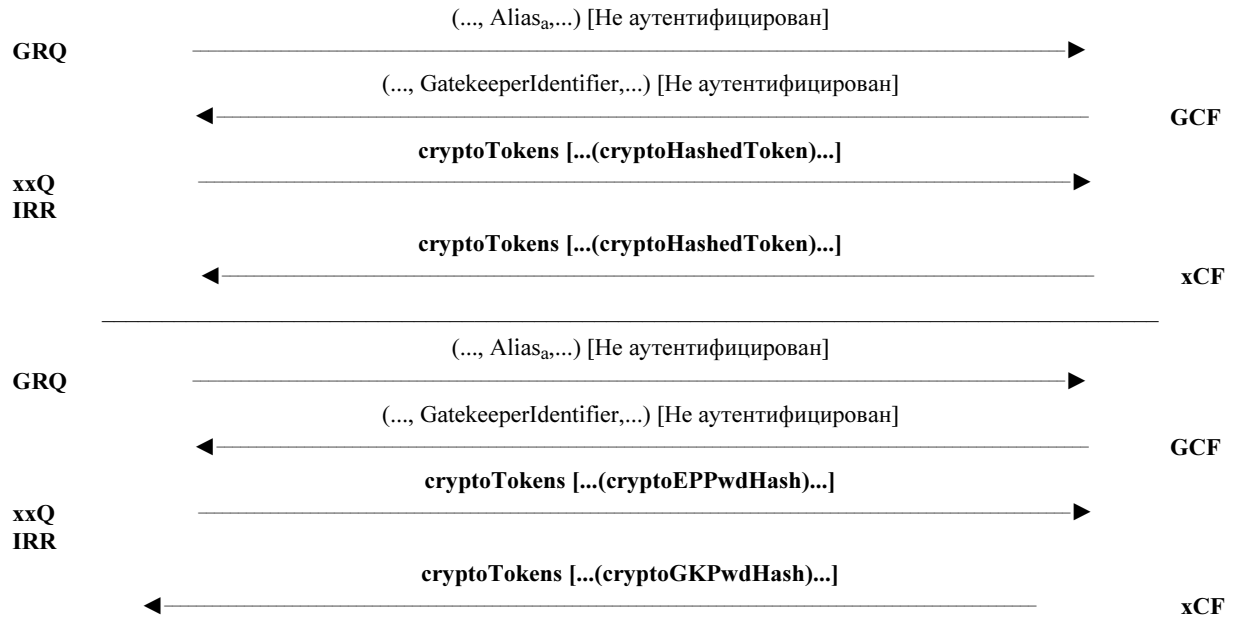


Рисунок 12/H.235.0 – Пароль с хэшированием

8.3.2.3 Вариант, основанный на сертификатах с подписями

Фаза обнаружения привратника (**GRQ**, **GCF** и **GRJ**) может быть незащищена, как показано на рисунке 13, или может быть защищена, согласно Рек. МСЭ-Т H.235.2, с использованием **cryptoTokens**.

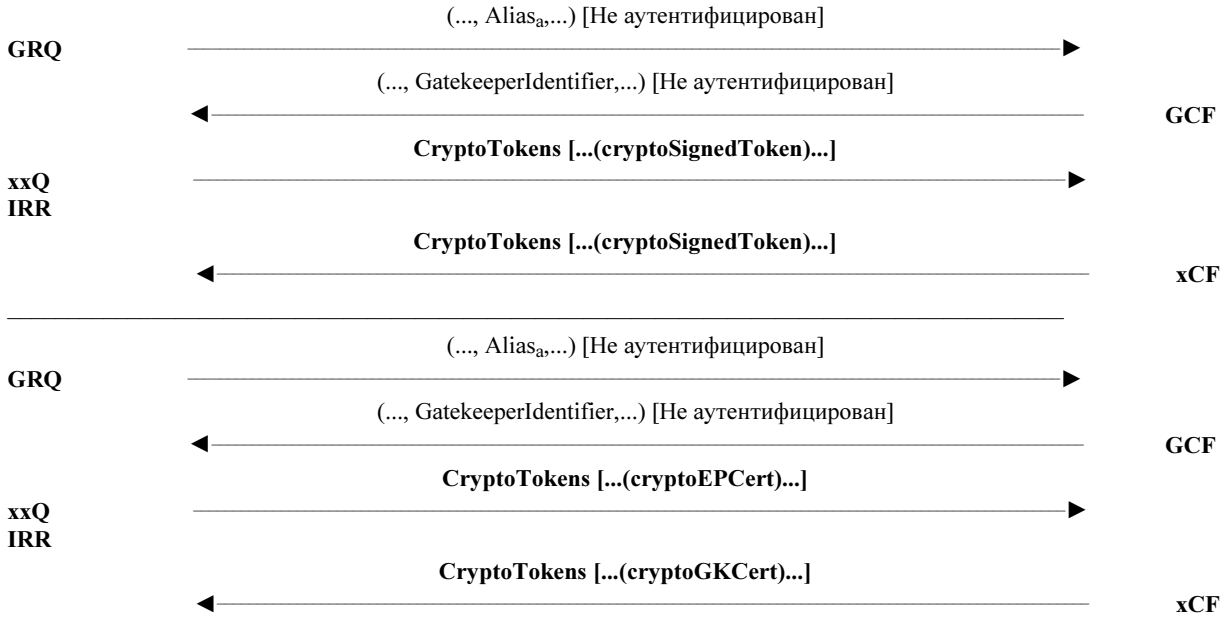


Рисунок 13/H.235.0 – Вариант, основанный на сертификатах с подписями

8.4 Управление ключом в канале RAS

При некоторых обстоятельствах желательно распространять (RAS) сеансовые ключи от привратника к одной или более конечным точкам под его контролем или от одной конечной точки к другой. В предложенном механизме предполагается, что привратник и конечная точка совместно используют сильный секретный ключ или знают открытые ключи друг друга. Одним из примеров такого случая может являться высылка маршрутизирующим привратником сеансового ключа конечной точке посредством сообщения RAS, как, например, **RCF** или **ACF**, для использования в шифровании маршрутизируемого привратником канала сигнализации. Другим примером может являться тот, в котором привратник высылает сеансовый ключ для использования в шифровании преуспевающих коммуникаций RAS (например, **RRQ** или **ARQ**).

Этот механизм похож на тот, который использовался в распространении сеансовых ключей медиа. Он может использоваться во избежание недостаточного согласования ключа при определенных обстоятельствах.

Для передачи ключа, в H.235v3 или выше должно использоваться дополнительное поле **h235Key ClearToken**. Гибкость элемента **H235Key** разрешит передачу материала шифровального ключа, используя:

- защищенный канал (опция **secureChannel**), предполагающий RAS, или канал сигнализации вызова защищается другими методами (IPsec/SSL и т. д.);
- общий секрет шифрования по чистому каналу (выбор **sharedSecret**) или подобный, но предпочтительный вариант **secureSharedSecret**;
- шифрование и сертификат открытого ключа по чистому каналу (выбор **certProtectedKey**).

Использование обменных сеансовых ключей RAS и их применение к RAS, сообщений сигнализации вызова и/или каналов передачи оставим для дальнейшего рассмотрения.

9 Ассиметричная аутентификация и обмен ключами с использованием систем шифрования эллиптической кривой

В данной Рекомендации предусмотрены утонченные методы с эллиптическими кривыми с применением к подписям, управлению ключом и шифрованию. Одними из главных преимуществ над "классическими" ассиметричными методами, как RSA, являются:

- Более короткие криптографические ключи, обеспечивающие сравнимую с RSA защиту: Характерные длины ключей для систем шифрования эллиптической кривой 160 битов; т. е. равные по защите 1024-битовым RSA ключам. Более короткий ключ потребляет меньше памяти для хранения, что делает системы шифрования эллиптической кривой особенно привлекательными для использования в смарт-картах и в любых других устройствах с низкими потребностями в памяти. В среде H.323 основанные на Приложении J/H.323 защищенные простые аудиотипы конечных точек (SASET), с их низкими ценовыми требованиями, хорошо подходят для осуществления методов с использованием эллиптической кривой.
- Увеличенное быстродействие достигается как в программных, так и в аппаратных реализациях: Более короткие ключи способствуют быстродействию. Это приводит к более быстрым интерактивным ответам (пользователей).

Всю вводную информацию, объяснение и процедуры обработки шифрования эллиптическими кривыми можно найти в *ATM Security Specification Version 1.1*, раздел 8.7. Рекомендуется шифровать эллиптические точки в их аффинной, несжатой нотации без использования метода точечной компрессии/декомпрессии. Более подробная информация по этой теме доступна в ИСО/МЭК 15946-1 и ИСО/МЭК 15946-2.

9.1 Управление ключом

Схемы реализации соглашения с ключом эллиптической кривой Диффи-Хеллмана похожи на классический случай mod-p, также описанный в этой Рекомендации. Есть два случая:

- эллиптические кривые в первичном поле: **eckasdhp** содержит эллиптическую кривую и параметры Диффи-Хеллмана;
- эллиптические кривые характеристики 2: **eckasdh2** содержит эллиптическую кривую и параметры Диффи-Хеллмана;

Структура ECKASDH содержит каждый из случаев. Некоторые примеры эллиптических кривых перечислены в ИСО/МЭК 15946-1. Также могут быть использованы любые другие подходящие эллиптические кривые.

Благодаря доступной последовательной структуре сигнализации **ClearToken**, как **dhkey**, так и **eckasdhkey** не должны возникать одновременно; когда применяется обмен ключами по Диффи-Хеллману, должен присутствовать только один из них.

Замечание – Не путайте случайно выбранные секретные параметры ***a*** из группы A или ***b*** из группы B с обычными коэффициентами Вейерштрасса ***a***, ***b***.

9.2 Цифровая подпись

Поле **ECGDSASignature** несет значения **r** и **s** вычисленной цифровой подписи, основанной на эллиптической кривой. Раздел 8.7.3 *ATM Security Specification Version 1.1* и глава 5 ИСО/МЭК 15946-2 предусматривают более подробную информацию по алгоритму подписей EC-GDSA.

Цифровая подпись, основанная на эллиптической кривой **ECGDSA**, должна быть кодирована посредством ASN.1 и затем помещена в поле **signature** макроса **SIGNED** этой Рекомендации. Для цифровой подписи посылающий должен включить идентификатор объекта в **algorithmOID**, по которому принимающий может определить использование цифровой подписи эллиптической кривой.

10 Псевдослучайная функция (PRF)

В этом пункте определяется псевдослучайная функция для целей получения динамических ключей из материала статического ключа и случайного значения.

ПРИМЕЧАНИЕ. – Эта PRF идентична MIKEY PRF (см. RFC 3830, раздел 4.1.2).

В методе получения ключа располагают следующими вводными параметрами:

- *inkey*: вводный ключ для функции получения.
- *inkey_len*: длина вводного ключа в битах.
- *label*: специфический ярлык, зависящий от типа получаемого ключа и случайного значения **challenge**.
- *outkey_len*: желательная длина получаемого ключа в битах.

Псевдослучайная функция на выходе имеет следующее:

- *outkey*: выходной ключ желательной длины.

Эта PRF должна использовать PRF, как указанная в RFC 3830, раздел 4.1.2.

11 Восстановление при ошибках защиты

В данной Рекомендации не указываются и не рекомендуются какие-либо методы, которыми конечные точки могут отследить свою абсолютную секретность. В ней, однако, рекомендуются действия, предпринимаемые, когда обнаружена потеря секретности.

Если одна из конечных точек обнаруживает брешь в защите канала установки соединения (например, H.225.0 для H.323), ей следует немедленно прекратить соединение, следуя протокольным процедурам, подходящим для отдельной конечной точки (для 8.5/H.323, за исключением шага B-5).

Если одна из конечных точек обнаруживает брешь в защите канала H.245 или логического канала защищенных данных (**h235Control**), ей следует немедленно прекратить соединение, следуя протокольным процедурам, подходящим для отдельной конечной точки (для 8.5/H.323 за исключением шага B-5).

Если конечная точка обнаруживает потерю секретности на одном из логических каналов, ей следует немедленно запросить новый ключ **(encryptionUpdateRequest)** и/или закрыть логический канал. В отделении MC(U) потеря секретности на одном логическом канале может привести к закрытию других логических каналов и/или повторному получению ключей в отделении MC(U). MC(U) должен посылать **encryptionUpdateRequest**, **encryptionUpdate** нескольким и всем затрагиваемым конечным точкам.

На усмотрение MC(U), ошибка защиты на отдельном канале может привести к прекращению соединений на всех конечных точках конференции, заканчивая, таким образом, конференцию.

11.1 Сигнализация ошибок

В способном к защите привратнике или другом улучшенном защитой объекте H.225.0 должны быть предусмотрены индикаторы ошибок. Ошибка защиты показывает, что объект не способен корректным образом обрабатывать полученное сообщение. Когда это возможно, должен быть предусмотрен подробный код ошибки.

- **securityWrongSyncTime** должен показывать, что отправитель нашел в защите проблему с несоответствием временных отметок. Она может возникать вследствие проблем с сервером времени, потери синхронизации или из-за чрезмерных задержек сети.
- **securityReplay** должен показывать, что была встречена атака воспроизведения. Это тот случай, когда одно и то же число последовательности возникает более чем единожды для данной временной отметки.
- **securityWrongGeneralID** должен показывать несовпадение основного ID в сообщении. Это может быть вызвано неправильной адресацией.
- **securityWrongSendersID** должен показывать несовпадение ID отправителя в сообщении. Это может быть вызвано ошибочным входом пользователя.
- **securityIntegrityFailed** должен показывать, что проверка на целостность/подпись не удалась. Для H.235.1 это может быть вызвано неправильным или с опечаткой паролем в ходе первоначального запроса или встреченной активной атакой. Для H.235.2 и H.235.3 он должен

показывать, что проверка цифровой подписи на сообщении не удалась. Это может быть вызвано неправильным применением частного/открытого ключа или встреченной активной атакой.

- **securityWrongOID** должен показывать любое несовпадение в OID маркеров (чистых или шифровальных маркеров) или OID алгоритма шифрования. Он показывает, что были использованы другие алгоритмы/профили.
- **securityDHmismatch** должен показывать любые несовпадения в обмениваемых параметрах Диффи-Хеллмана. Он может показывать, что используются другие наборы параметров DH или даже другие алгоритмы голосового шифрования.
- **securityCertificateExpired** должен показывать, что сертификат устарел.
- **securityCertificateDateInvalid** должен показывать, что сертификат пока еще не действителен.
- **securityCertificateRevoked** должен показывать, что сертификат был обнаружен недействительным.
- **securityCertificateNotReadable** должен показывать, что сертификат не может быть корректно расшифрован ASN.1 или имеет другую плохую форму.
- **securityCertificateSignatureInvalid** должен показывать, что подпись на сертификате не верна.
- **securityCertificateMissing** должен показывать, что сертификат ожидался, но не был найден или, что сертификат невозможно обнаружить по другим причинам.
- **securityCertificateIncomplete** должен показывать, что отсутствовали некоторые ожидаемые расширения сертификата
- **securityUnsupportedCertificateAlgOID** должен показывать, что определенные алгоритмы шифрования, такие как цифровые подписи или хэширование, использованные внутри сертификата, не поняты или не поддерживаются. Как часть возвращаемого ответа, отправитель может обеспечить список приемлемых сертификатов в отдельных маркерах с целью способствовать выбору подходящего получателем.
- **securityUnknownCA** должен показывать, что сертификат CA/root невозможно было обнаружить или что сертификат не мог совпадать с доверенным CA.

В любом другом случае, когда функционирование системы защиты H.235 терпит неудачу, должен возвращаться **securityDenial** для RAS H.225.0 (**securityDenied** для сигнализации вызова H.225.0, соответственно).

ПРИМЕЧАНИЕ 1. – securityWrongSyncTime, securityReplay, securityWrongGeneralID, securityWrongSendersID, SecurityIntegrityFailed, securityDHmismatch и securityWrongOID могут возникать в профилях защиты H.235.1, H.235.2 или H.235.3.

ПРИМЕЧАНИЕ 2. – securityCertificateExpired, securityCertificateDateInvalid, securityCertificateRevoked, securityCertificateNotReadable, securityCertificateSignatureInvalid, securityCertificateMissing, securityCertificateIncomplete, securityUnsupportedCertificateAlgOID и securityUnknownCA могут возникать в профилях защиты H.235.2 или H.235.3.

Приложение A

H.235 ASN.1

```
H235-SECURITY-MESSAGES DEFINITIONS AUTOMATIC TAGS::=
BEGIN

-- EXPORTS All

ChallengeString         ::= OCTET STRING (SIZE(8..128))
TimeStamp               ::= INTEGER(1..4294967295)     -- секунды начиная с 00:00
                                                       -- 1/1/1970 UTC
RandomVal               ::= INTEGER -- 32-bit Integer
Password                ::= BMPString (SIZE (1..128))
Identifier              ::= BMPString (SIZE (1..128))
KeyMaterial             ::= BIT STRING(SIZE(1..2048))

NonStandardParameter::= SEQUENCE
{
     nonStandardIdentifier   OBJECT IDENTIFIER,
     data                    OCTET STRING
}

-- если используются локальнаые представления этих битовых строк, они должны
-- использовать стандартный порядок сетевых октетов (например, Big Endian)
DHset::= SEQUENCE
{
     halfkey       BIT STRING (SIZE(0..2048)), -- = g^x mod n
     modSize       BIT STRING (SIZE(0..2048)), -- n
     generator     BIT STRING (SIZE(0..2048)), -- g
     ...
}

ECpoint::= SEQUENCE -- несжатое (x, y) аффинное координатное представление
                    -- точек эллиптической кривой
{
     x         BIT STRING (SIZE(0..511)) OPTIONAL,
     y         BIT STRING (SIZE(0..511)) OPTIONAL,
     ...
}

ECKASDH::= CHOICE – параметры для схемы реализации соглашения с ключом
эллиптической кривой Диффи-Хеллмана
{
     eckasdhp SEQUENCE – параметры для эллиптических кривых первичного поля
     {
          public-key    ECpoint, -- Это поле содержит представление значения
               -- открытого ключа ECKAS-DHp. Это поле содержит значение (aP)
               -- открытого ключа инициатора ECKAS-DHp, когда этот элемент данных
               -- посылается от источника к получателю. Это поле содержит
               -- значение (bP) открытого ключа ответчика ECKAS-DHp, когда этот
               -- элемент данных посылается обратно от получателя к источнику
          modulus       BIT STRING (SIZE(0..511)), -- Это поле содержит
               -- представление значения (p) открытого модуля ECKAS-DHp.
          base          ECpoint, -- Это поле содержит преставление открытой базы
               -- (P) ECKAS-DHp.
          weierstrassA  BIT STRING (SIZE(0..511)), -- Это поле содержит
               -- представление коэффициента Вейерштрасса (a) ECKAS-DHp
          weierstrassB  BIT STRING (SIZE(0..511)) -- Это поле содержит
               -- представление коэффициента Вейерштрасса (b) ECKAS-DHp

     },
```

```
     eckasdh2 SEQUENCE -- параметры для эллиптических кривых характеристики 2
     {
          public-key    ECpoint, -- Это поле содержит представление значения
               -- открытого ключа ECKAS-DH2. Это поле содержит значение (aP)
               -- открытого ключа инициатора ECKAS-DH2, когда этот элемент данных
               -- посылается от источника к получателю. Это поле содержит
               -- значение (bP) открытого ключа ответчика ECKAS-DH2, когда этот
               -- элемент данных посылается обратно от получателя к источнику

          fieldSize     BIT STRING (SIZE(0..511)), -- Это поле содержит
               -- представление значения (m) размера поля ECKAS-DH2.
          base          ECpoint, -- Это поле содержит преставление открытой базы
               -- (P) ECKAS-DH2.

          weierstrassA  BIT STRING (SIZE(0..511)), -- Это поле содержит
               -- представление коэффициента Вейерштрасса (a) ECKAS-DH2
          weierstrassB  BIT STRING (SIZE(0..511)) -- Это поле содержит
               -- представление коэффициента Вейерштрасса (b) ECKAS-DH2
     },
     ...
}

ECGDSASignature::= SEQUENCE -- параметры для алгоритма цифровой подписи
               -- эллиптической кривой
{
     r         BIT STRING (SIZE(0..511)), -- Это поле содержит представление
               -- компонента r цифровой подписи ECGDSA
     s         BIT STRING (SIZE(0..511)) -- Это поле содержит представление
               -- компонента s цифровой подписи ECGDSA
}

TypedCertificate::= SEQUENCE
{
     type           OBJECT IDENTIFIER,
     certificate    OCTET STRING,
     ...
}

AuthenticationBES::= CHOICE

{
     default        NULL, -- шифрованный ClearToken
     radius         NULL, -- RADIUS-запрос/ответ
     ...

}

AuthenticationMechanism ::= CHOICE
{
     dhExch         NULL, -- Диффи-Хеллман
     pwdSymEnc      NULL, -- пароль с симметричным шифрованием
     pwdHash        NULL, -- пароль с хэшированием
     certSign       NULL, -- сертификат с подписью
     ipsec          NULL, -- соединение, основанное на IPSEC
     tls            NULL,
     nonStandard    NonStandardParameter, -- что-то еще.
     ...,
     authenticationBES  AuthenticationBES, -- аутентификация пользователя для  BES
     keyExch   OBJECT IDENTIFIER – профиль обмена ключами
}
```

```
ClearToken          ::= SEQUENCE -- "маркер" может содержать несколько типов значений.
{
     tokenOID       OBJECT IDENTIFIER,
     timeStamp      TimeStamp OPTIONAL,
     password       Password OPTIONAL,
     dhkey          DHset OPTIONAL,
     challenge      ChallengeString OPTIONAL,
     random         RandomVal OPTIONAL,
     certificate    TypedCertificate OPTIONAL,
     generalID      Identifier OPTIONAL,
     nonStandard    NonStandardParameter OPTIONAL,
     ...,
     eckasdhkey     ECKASDH OPTIONAL,  -- Аналог схемы реализации соглашения с
                                       -- ключом эллиптической кривой
                                       -- Диффи-Хеллмана (ECKAS-DH)
     sendersID      Identifier OPTIONAL,
     h235Key        H235Key OPTIONAL, -- центральный распространяемый ключ в V3
     profileInfo    SEQUENCE OF ProfileElement OPTIONAL -- специфика профиля
}

--   Идентификатор объекта следует поместить в поле tokenOID, когда
--   ClearToken напрямую включен в сообщение (как противоположный
--   шифруемому). Во всех остальных случаях, приложению следует использовать
--   идентификатор объекта { 0 0 }, чтобы показать, что значение маркера
--   tokenOID отсутствует.
--   Начнем описывать все криптографически параметризованные типы здесь...
--

ProfileElement      ::= SEQUENCE
{
     elementID      INTEGER (0..255),  -- идентификатор элемента, как определено
                                       -- профилем
     paramS         Params OPTIONAL,   -- любые параметры специфики элементов
     element        Element OPTIONAL,  -- в требуемой форме
     …
}

Element::= CHOICE
{
     octets             OCTET STRING,
     integer            INTEGER,
     bits               BIT STRING,
     name               BMPString,
     flag               BOOLEAN,
     …
}



SIGNED { ToBeSigned }::= SEQUENCE {
     toBeSigned         ToBeSigned,
     algorithmOID       OBJECT IDENTIFIER,
     paramS             Params,   -- любые параметры "рабочего цикла"
     signature          BIT STRING -- может быть шифрованная RSA или ASN.1
подпись ECGDSA
} ( CONSTRAINED BY { -- проверить или подтвердить сертификат -- } )


ENCRYPTED { ToBeEncrypted }::= SEQUENCE {
     algorithmOID       OBJECT IDENTIFIER,
     paramS             Params,   -- любые параметры "рабочего цикла"
     encryptedData      OCTET STRING
} ( CONSTRAINED BY { -- шифровать или дешифровать -- ToBeEncrypted } )
```

```
HASHED { ToBeHashed }::= SEQUENCE {
     algorithmOID       OBJECT IDENTIFIER,
     paramS             Params,   -- любые параметры "рабочего цикла"
     hash               BIT STRING
} ( CONSTRAINED BY { -- Hash -- ToBeHashed } )

IV8::= OCTET STRING (SIZE(8)) -- начальные значения 64-битовых блоковых шифров
IV16::= OCTET STRING (SIZE(16)) -- начальные значения 128-битовых блоковых шифров

-- в используемом алгоритме подписи нужно выбрать один из этих типов параметров,
-- необходимых для получения окончания подписи.

Params::= SEQUENCE {
     ranInt         INTEGER OPTIONAL, -- какое-то целое значение
     iv8            IV8 OPTIONAL, -- 8-октетный вектор инициализации
     ...,
     iv16           IV16 OPTIONAL,-- 16-октетный вектор инициализации
     iv             OCTET STRING OPTIONAL, -- вектор инициализации произвольной
      -- длины
     clearSalt      OCTET STRING OPTIONAL -- нешифрованный расширяющий (salting)
     ключ для шифрования
}

EncodedGeneralToken::= TYPE-IDENTIFIER.&Type (ClearToken -- основной
используемый маркер -- )
PwdCertToken::= ClearToken (WITH COMPONENTS {..., timeStamp PRESENT, generalID
PRESENT})
EncodedPwdCertToken::= TYPE-IDENTIFIER.&Type (PwdCertToken)

CryptoToken::= CHOICE
{

     cryptoEncryptedToken SEQUENCE -- основной маркер специфики целей/применения
     {
          tokenOID  OBJECT IDENTIFIER,
          token          ENCRYPTED { EncodedGeneralToken }
     },
     cryptoSignedToken SEQUENCE -- основной маркер специфики целей/применения
     {
          tokenOID  OBJECT IDENTIFIER,
          token          SIGNED { EncodedGeneralToken }
     },
     cryptoHashedToken SEQUENCE -- основной маркер специфики целей/применения
     {
          tokenOID       OBJECT IDENTIFIER,
          hashedVals          ClearToken,
          token HASHED { EncodedGeneralToken }
     },
     cryptoPwdEncr ENCRYPTED { EncodedPwdCertToken },
     ...
}

-- Они делают возможным прохождение сеансовых ключей внутри структуры H.245 OLC.
-- Они шифруются как отдельностоящие ASN.1 и основанные на OCTET STRING внутри
-- H.245
H235Key   ::=CHOICE -- Используется с H.245 или полем "h235Key" ClearToken
{
     secureChannel           KeyMaterial,
     sharedSecret            ENCRYPTED {EncodedKeySyncMaterial},
     certProtectedKey        SIGNED {EncodedKeySignedMaterial },
```

```
     ...,
     secureSharedSecret      V3KeySyncMaterial -- для конечных точек V3 H.235
}

KeySignedMaterial::= SEQUENCE {
     generalId      Identifier, -- псевдоним ведомого
     mrandom        RandomVal, -- случайное значение ведущего
     srandom        RandomVal OPTIONAL, -- случайное значение ведущего
     timeStamp      TimeStamp OPTIONAL, -- временная отметка ведущего для
     добровольного EU
     encrptval      ENCRYPTED { EncodedKeySyncMaterial }
}
EncodedKeySignedMaterial::= TYPE-IDENTIFIER.&Type (KeySignedMaterial)

H235CertificateSignature     ::= SEQUENCE
{
     certificate             TypedCertificate,
     responseRandom          RandomVal,
     requesterRandom         RandomVal OPTIONAL,
     signature               SIGNED { EncodedReturnSig },
     ...
}

ReturnSig::= SEQUENCE {
     generalId               Identifier, -- псевдоним ведущего
     responseRandom          RandomVal,
     requestRandom           RandomVal OPTIONAL,
     certificate             TypedCertificate OPTIONAL -- запрошенный сертификат
}

EncodedReturnSig::= TYPE-IDENTIFIER.&Type (ReturnSig)
KeySyncMaterial    ::= SEQUENCE
{
     generalID      Identifier,
     keyMaterial    KeyMaterial,
     ...
}
EncodedKeySyncMaterial  ::=TYPE-IDENTIFIER.&Type (KeySyncMaterial)



V3KeySyncMaterial  ::= SEQUENCE
{
     generalID               Identifier OPTIONAL, -- ID равной конечной точки
     algorithmOID            OBJECT IDENTIFIER OPTIONAL, -- алгоритм шифрования
     paramS                  Params, -- IV
     encryptedSessionKey     OCTET STRING OPTIONAL, -- шифрованный сеансовый
 -- ключ
     encryptedSaltingKey     OCTET STRING OPTIONAL, -- шифрованный
                                                    -- расширяющий ключ медиа
     clearSaltingKey         OCTET STRING OPTIONAL, -- нешифрованный
                                                    -- расширяющий ключ медиа
     paramSsalt              Params OPTIONAL, -- IV (и чистое расширение (salt))
                                                    -- для расширения (salting)
                                                    -- шифрования ключа
     keyDerivationOID        OBJECT IDENTIFIER OPTIONAL, -- метод получения ключа
     ...,
     genericKeyMaterial      OCTET STRING OPTIONAL -- форма материала ключа
                         -- шифрованного ASN.1 зависит от связанного с ним
                         -- шифровального тега медиа

}


END  -- КОНЕЦ ОПРЕДЕЛЕНИЙ СООБЩЕНИЙ ЗАЩИТЫ H235
```

Приложение B

Особые вопросы H.324

Для дальнейшего изучения.

Дополнение I

Подробности реализации в H.323

I.1 Примеры реализации

В следующих подпунктах описаны примеры реализаций, которые могут быть разработаны внутри инфраструктуры H.235. Они не нацелены заключить в себе множество других возможностей, доступных внутри этой Рекомендации, а скорее нацелены дать более конкретные примеры использования внутри Рек. МСЭ-Т H.323.

I.1.1 Маркеры

В этом пункте описан пример использования маркеров защиты для скрытия информации адресации в место назначения. Сценарий примера: конечная точка, желающая сделать вызов другой конечной точки, используя ее хорошо известный псевдоним. А именно, он содержит конечную точку H.323, привратник, POTS-шлюз и телефон, как изображено на рисунке I.1.

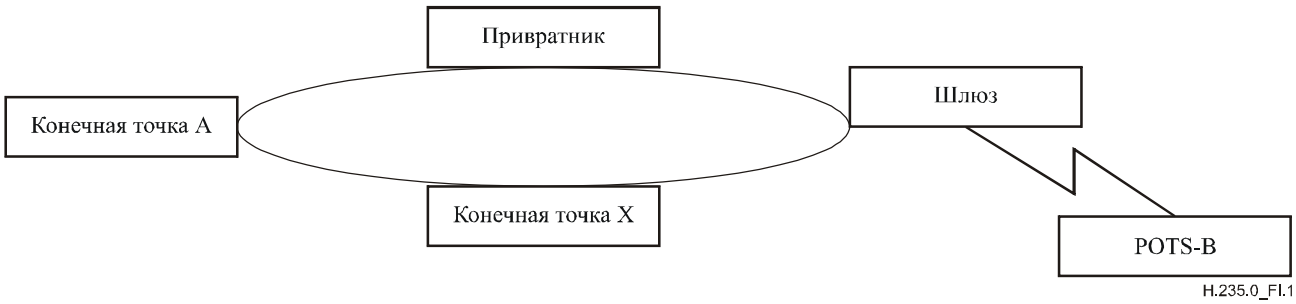


Рисунок I.1/H.235.0 – Маркеры

На настоящий момент H.323 может функционировать способом, подобным телефонной сети с ID звонящего. В этом сценарии будет проиллюстрирована ситуация, в которой *звонящий* не хочет раскрывать свой физический адрес, при этом позволяя вызову завершиться. Это может быть важным в шлюзах POTS-H.323, где может быть необходимым оставлять телефон назначения секретным.

Допустим, что EPA пытается позвонить POTS-B и POTS-B не хочет раскрывать свой E.164 телефонный номер EPA. (То, каким образом осуществляется эта установка, выходит за рамки этого примера.)

- EPA пошлет **ARQ** своему привратнику, чтобы узнать адрес телефона POTS, как представленного его псевдонимом/шлюзом. Привратник узнал бы его как "частный" псевдоним, зная, что для того чтобы совершить соединение, он должен сообщить адрес шлюза POTS (аналогично возвращению адреса шлюза H.320, если конечная точка H.320 вызывается конечной точкой H.323).
- В возвращаемом **ACF** привратник возвращает адрес шлюза POTS, как и ожидалось. Информация адресации, требуемая, чтобы дозвониться до конечного телефона (т. е. телефонный номер), возвращается в зашифрованный маркер, включенный в **ACF**. Этот

зашифрованный маркер содержит фактический E.164 (телефонный номер) телефона, который не может быть дешифрован и понят звонящим (т. е. EPA).

- Конечная точка высылает сообщение SETUP устройству шлюза (чей адрес сигнализации вызова был возвращен в **ACF**), включая непрозрачный маркер(ы), который она получила с **ACF**.
- Шлюз, при получении SETUP, высылает свой **ARQ** своему привратнику, включая любой маркер(ы), который был получен в SETUP.
- Привратник способен дешифровать маркер(ы) и возвращает телефонный номер в **ACF**.

Часть ASN.1 структуры маркера примера показана ниже, с описанием содержимого полей. Предположим, мы используем **cryptoEncodedGeneralToken** для содержания шифрованного телефонного номера.

В реализации может быть выбран **tokenOID** и обозначен, как содержащий телефонный номер E.164. Особый метод, используемый для шифрования этого телефонного номера (например, 56-битовый DES), был бы включен в определение "ENCRYPT" **algorithmOID**.

```
CryptoToken::= CHOICE
{
     cryptoEncodedGeneralToken SEQUENCE     -- основной маркер специфики
                                            -- целей/применения
     {
          tokenOID OBJECT IDENTIFIER,
          ENCRYPTED { EncodedGeneralToken }
     },
.
.
. [abbreviated text]
.

}
```

CryptoToken мог бы проходить в сообщениях SETUP (из EPA в шлюз) и **ARQ** (от шлюза к привратнику), как обозначено выше. Поле того как привратник дешифровал маркер (телефонный номер), он бы передал его чистую версию в **clearToken**.

I.1.2 Использование маркеров в системах H.323

Существовала некая неразбериха в использовании **CryptoH323Tokens**, как проходящих в сообщениях RAS. Существуют две главных категории **CryptoH323Tokens**: используемые для процедур H.235 и используемые способом специфических приложений. Использовать эти маркеры следует, согласно следующим правилам:

- Все определенные H.235 (например, **cryptoEPPwdHash**, **cryptoGKPwdHash**, **cryptoEPPwdEncr**, **cryptoGKPwdEncr**, **cryptoGKCert** и **cryptoFastStart**) должны быть использованы в процедурах и алгоритмах, как описанные в этой Рекомендации.
- При основанном на специфике приложений или собственническом использовании маркеров нужно использовать **nestedcryptoToken** для их обменов.
- Любой используемый **nestedcryptoToken** должен иметь **tokenOID** (объектный идентификатор), который недвусмысленно идентифицирует его.

I.1.3 Использование случайных значений H.235 в системах H.323

Случайное значение, которое проходит в последовательности **xRQ**/**xCF** между конечными точками и привратниками, может быть обновлено привратником. Как было описано в 8.3.1, это случайное значение может быть обновлено в любом сообщении **xCF**, чтобы быть использованным в последующих сообщениях **xRQ** из конечной точки. Вследствие того, что сообщения RAS могут быть утеряны (включая **xCF**/**xRJ**), обновленное случайное значение также может быть утеряно. Выходом из этой ситуации может быть реинициализация контекста защиты, но это оставлено для локальной реализации.

Реализации, в которых требуется использование множества видных запросов RAS, будут ограничены обновлением случайных значений, используемых в любой аутентификации. Если обновление этих значений происходит при каждом ответе на запрос, параллельные запросы невозможны. Одним из возможных решений является содержание логического "окна", в течение которого случайное значение остается постоянным. Такой исход является предметом локальной реализации.

I.1.4 Пароль

В этом примере предполагается, что пользователь является абонентом привратника (т. е. пользователь будет находиться в его зоне) и имеет соответствующий ID подписи и пароль. Пользователь зарегистрировался бы у привратника, используя ID подписи (как проходящий в псевдониме – H323ID) и шифруя строку запроса, предоставленную привратником. Это предполагает, что привратник также знает пароль, относящийся к ID подписи. Привратник аутентифицирует пользователя, убедившись, что строка запроса была правильно зашифрована.

Примером процедуры регистрации с аутентификацией привратником является следующее:

1) Если конечная точка будет использовать **GRQ** для обнаружения привратника, одним из псевдонимов в сообщении являлся бы ID подписи (как **H323ID**). **authenticationcapability** содержал бы **AuthenticationMechanism** в **pwdSymEnc,** и **algorithmOIDs** были бы установлены на указание всего набора алгоритмов, поддерживаемых конечной точкой. (К примеру, одним из них мог бы являться 56-битовый DES в режиме ECB.)

2) Привратник ответил бы с помощью **GCF** (допуская, что узнает псевдоним), несущего элемент **tokens**, содержащий один **ClearToken**. Этот **ClearToken** содержал бы как **challenge**, так и элемент **timeStamp**. **challenge** содержал бы 16 октетов. (Чтобы предупредить атаки воспроизведения, **ClearToken** должен содержать **timeStamp**.) **authenticationmode** следует установить на **pwdSymEnc** и **algorithmOID** следует установить на указание шифровального алгоритма, требуемого привратником (к примеру, 56-битовый DES в режиме ECB).

   Если привратник не поддерживает какого-либо **algorithmOIDs**, указанного в **GRQ**, тогда он ответил бы **GRJ**, содержащим **GatekeeperRejectReason** в **resourceUnavailable**.

3) Конечной точке следовало бы затем зарегистрироваться у (одного из) привратника (привратников), ответившего **GCF**, послав **RRQ**, содержащий **cryptoEPPwdEncr** в **cryptoTokens**. **cryptoEPPwdEncr** имел бы **algorithmOID** шифровального алгоритма, с которым было соглашено в обмене **GRQ**/**GCF**, и зашифрованный запрос.

   Ключ шифрования собирается из пароля пользователя с использованием процедуры, описанной в 8.2.1. Полученная в результате "строка" октетов затем используется в качестве ключа DES для шифрования **challenge**.

4) Когда привратник получит зашифрованный запрос в **RRQ**, она сравнила бы его с таким же образом генерированным зашифрованным запросом, чтобы аутентифицировать регистрирующегося пользователя. Если две зашифрованных строки не совпадут, привратник ответил бы **RRJ** с **RegistrationRejectReason**, установленным в **securityDenial**, или другим подходящим кодом ошибки защиты, согласно пункту 11.1. Если они совпадают, привратник посылает **RCF** конечной точке.

5) Если привратник получит **RRQ**, который не содержит приемлемого элемента **cryptoTokens**, тогда ему следует ответить **RRJ** с **GatekeeperRejectReason** в **discoveryRequired**. Конечная точка при получении такого **RRJ** может выполнить обнаружение, которое позволит привратнику/конечной точке обменять новый запрос.

   ПРИМЕЧАНИЕ. – Сообщение GRQ может являться одноадресным для привратника.

I.1.5 IPsec

В основном, IPsec ([RFC 2401], RFC 2406 [ESP]) и RFC 2409 [IKE] может использоваться для аутентификации и, дополнительно, для конфиденциальности (т. е. шифрования) на уровне IP, прозрачном для любого работающего над ним протокола (приложения). Чтобы допустить это, не нужно обновлять протокол приложения; только правила защиты в каждом конце.

Например, чтобы максимально использовать IPsec для простого вызова точка-точка, можно следовать следующему сценарию:

1) Осуществляющая вызов конечная точка и ее привратник установили бы правило требовать использования IPsec (аутентификации и, дополнительно, конфиденциальности) в протоколе RAS. Так, перед тем как первое сообщение RAS будет послано от конечной точки к привратнику, демон ISAKMP (RFC 2407)/Oakley (RFC 2412) в конечной точке согласует услуги защиты для использования в пакетах 'в' и 'из' известного порта канала RAS. Как только согласование будет завершено, канал RAS будет функционировать в точности, как если бы он не был защищен. С использованием этого защищенного канала привратник проинформирует конечную точку об адресе и номере порта канала сигнализации вызова к вызываемой точке.

2) После получения адреса и номера порта канала сигнализации вызова осуществляющая вызов конечная точка динамично обновила бы свои правила защиты, чтобы требовать желательную защиту IPsec по этому адресу и паре протокол/порт. Теперь, когда осуществляющая вызов конечная точка будет пытаться соединиться с этим адресом/портом, пакеты выстраивались бы в очередь, в то время как выполнялось бы согласование ISAKMP (RFC 2407)/Oakley (RFC 2412) между конечными точками. При выполнении этого согласования для адреса/порта будет существовать ассоциация защиты IPsec (SA) и может происходить сигнализация Q.931.

3) В обмене Q.931 SETUP и CONNECT конечные точки могут согласовать использование IPsec для канала H.245. Это позволит конечным точкам снова динамично обновлять их базы данных правил IPsec, чтобы форсировать использование IPsec в этом соединении.

4) Как с каналом сигнализации вызова, транспарентное согласование ISAKMP (RFC 2407)/Oakley (RFC 2412) будет иметь место перед тем, как будут переданы любые пакеты H.245. Аутентификация, осуществляемая в этом обмене ISAKMP (RFC 2407)/Oakley (RFC 2412), будет первоначальной попыткой аутентификации пользователя пользователем и установит (вероятный) защищенный канал между двумя пользователями, на котором согласуются характеристики аудиоканала. Если после межперсональных вопросов-ответов какой-либо из пользователей не удовлетворен аутентификацией, можно выбрать другие сертификаты и повторить обмен ISAKMP (RFC 2407)/Oakley (RFC 2412).

5) После каждой аутентификации H.245 ISAKMP (RFC 2407)/Oakley (RFC 2412) происходит обмен новым шифровальным материалом для аудиоканала RTP. Этот шифровальный материал распространяется владельцем защищенного канала H.245. Поскольку протоколом H.245 владельцу определяется распространение шифровального материала медиа по каналу H.245 (чтобы допустить многоточечную связь), в этом канале RTP не рекомендуется использовать IPsec.

Шифрованный канал H.245 является потенциальной проблемой для прокси и сетевого экрана NAT с момента, когда протокол H.245 несет в себе динамически присваиваемые номера портов. Таким сетевым экранам придется дешифровать, видоизменять и перешифровывать протокол для корректного функционирования. По этой причине в Рек. МСЭ-Т H.245 был введен "Защищенный" логический канал. Если этот канал используется, канал H.245 может оставаться незащищенным; аутентификация и генерация ключей будет осуществляться "защищенным" логическим каналом. Сигнализация логического канала позволила бы этому каналу быть защищенным посредством IPsec, и секретный ключ, используемый в "Защищенном" логическом канале, использовался бы для защиты **EncryptionSync**, распространяемого владельцем канала H.245.

I.1.6 Поддержка серверных служб (BES)

Серверы служб являются важной дополнительной функцией всей, основанной на H.323, мультимедийной среды. Например, BES обеспечивает услуги для аутентификации пользователей, для авторизации, а также для создания учетных записей, записей долгов и счетов и других услуг. В простой модели такие услуги может обеспечить привратник. В разделенной архитектуре привратник не всегда может обеспечивать такие услуги также потому, что он может не иметь доступа к базам данных BES или может являться частью другого административного домена. Более того, оконечное устройство или пользователь обычно не знает их BES.

На рисунке I.2 показан сценарий с мультимедийным оконечным устройством (например, SASET), привратником и присоединенной BES. В рамки обзора Рек. МСЭ-Т H.323 не попадает то, как именно BES связывается с привратником. Могут применяться несколько методов и протоколов: RADIUS (см. RFC 2865) считается одним из самых важных, широко применяемых поставщиками услуг.

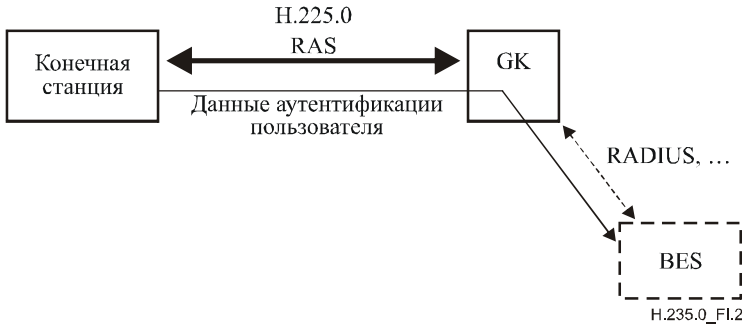


Рисунок I.2/H.235.0 – Сценарий с сервером служб

Привратник, предлагающий поддержку BES, должен предлагать, по меньшей мере, два следующих режима:

1) **режим "по умолчанию"**: в этом режиме оконечное устройство не знает BES и требует доверительных отношений с привратником. Оконечное устройство посылает данные аутентификации пользователя в зашифрованной форме (**cryptoEncryptedToken**). Привратник, который дешифрует их, извлекает информацию аутентификации и обращается с ней к BES. Основанное на пароле шифрование **ClearToken** совершается с применением отдельного секрета, который совместно используется оконечным устройством и привратником через **CryptoToken**. Шифровальный ключ может быть получен из пароля, с которым оконечное устройство безопасно регистрируется у привратника.

   CryptoToken несет **cryptoEncryptedToken**, где **tokenOID** установлен в "M", показывая режим "по умолчанию" BES; и **token**, содержащую:

   - **algorithmOID**, показывающий алгоритм шифрования; "Y" (DES56-CBC), "Z" (3DES-OCBC); см. пункт 11/H.235.6;
   - **paramS** не используется;
   - **encryptedData** установлен в октетное представление зашифрованного **ClearToken**.

   ClearToken содержит как **password** данные идентификации пользователя. Защищенной информацией **ClearToken** может быть пароль/PIN, опознавательная информация пользователя, номер карты предоплаты и номер кредитной карты. **timestamp** устанавливается на текущее время оконечного устройства, **random** содержит число монотонно возрастающей последовательности, **sendersID** устанавливается на ID оконечного устройства, **generalID** на идентификатор привратника. Начальное значение алгоритма шифрования должно оставаться постоянным; оно может являться частью секрета подписи оконечного устройства.

   ПРИМЕЧАНИЕ. – **ClearToken** не передается.

2) **режим RADIUS**: в этом режиме BES и пользователь оконечного устройства совместно используют общий секрет, и привратнику не следует доверять посредством аутентификации RADIUS BES. Привратник просто переадресовывает запрос RADIUS, полученный от BES в процессе *доступа-запроса* по направлению к оконечному устройству, и посылает ответ пользователя как ответ RADIUS в процессе *доступа-запроса* в обратном направлении. Оконечное устройство и привратник согласуют эту возможность запроса/ответа **radius** в **AuthenticationBES** внутри **AuthenticationMechanism** в процессе обнаружения привратника.

   В процессе приема сообщения RADIUS *доступа-запроса*, содержащего запрос, привратник помещает 16-октетный запрос в поле **challenge ClearToken**, когда запрашивает у оконечного устройства **GCF** или любое другое сообщение RAS. 'K' **tokenOID** в **ClearToken** показывает запрос RADIUS.

Затем оконечное устройство может представить запрос пользователю и ждать, пока будет введен ответ. Оконечное устройство должно ответить сообщением RAS, в котором ответ помещается в поле **challenge ClearToken**. 'L' **tokenOID** в **ClearToken** показывает ответ RADIUS.

В таблице I.1 перечислены все упомянутые OID.

Таблица I.1/H.235.0 – Идентификаторы объектов, используемые I.1.6

Ссылка на идентификатор объекта	Значение идентификатора объекта	Описание
"K"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 31}	Показывает запрос RADIUS в ClearToken
"L"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 32}	Показывает ответ RADIUS (содержащийся в поле запроса) в ClearToken
"M"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 33}	Показывает режим "по умолчанию" BES с защищенным паролем в ClearToken

Дополнение II

Подробности реализации в H.324

Для дальнейшего изучения.

Дополнение III

Другие подробности реализации серии H

Для дальнейшего изучения.

Дополнение IV

Соответствие разделов H.235v3Amd1Cor1 подсерии Рекомендаций H.235v4

В этом информационном Дополнении приведено положение всех разделов H.235v3Amd1Cor1 внутри подсерии Рекомендаций H.235v4.

Таблица IV.1/H.235.0 – Соответствие пунктов

Пункт H.235v3Amd1Cor1	Название	Подсерия Рекомендаций H.235v4.x	Пункт
Основная часть	–	–	–
1	Сфера применения	H.235.0	1
2	Справочные документы	H.235.0	2
		H.235.1	2
		H.235.2	2
		H.235.3	2
3	Термины и определения	H.235.0	3
		H.235.2	3
		H.235.6	3
4	Символы и сокращения	H.235.0	4
		H.235.3	4
		H.235.6	4
5	Соглашения по терминам	H.235.0	5
		H.235.2	5
		H.235.6	5
6	Введение в систему	H.235.0	6
6.1	Резюме	H.235.0	6.1
6.2	Аутентификация	H.235.0	6.2
6.2.1	Сертификаты	H.235.0	6.2.1
6.3	Защита осуществления вызова	H.235.0	6.3
6.4	Защита контроля вызова (H.245)	H.235.0	6.4
6.5	Секретность потока медиа	H.235.0	6.5
6.6	Защитные элементы	H.235.0	6.6
6.6.1	Условное депонирование ключа	H.235.0	6.6.1
6.7	Невозможность отказа	H.235.0	6.7
6.8	Конфиденциальность подвижной связи	H.235.0	6.8
6.9	Профили защиты	H.235.0	6.9
7	Процедуры осуществления соединения	H.235.0	7
7.1	Введение	H.235.0	–
8	Сигнализация и процедуры H.245	H.235.6	7

Таблица IV.1/H.235.0 – Соответствие пунктов

Пункт H.235v3Amd1Cor1	Название	Подсерия Рекомендаций H.235v4.x	Пункт
8.1	Защищенная работа канала H.245	H.235.6	7.1
8.2	Незащищенная работа канала H.245	H.235.6	7.2
8.3	Обмен возможностями	H.235.6	7.3
8.4	Роль ведущего	H.235.6	7.4
8.5	Сигнализация логического канала	H.235.6	7.5
8.6	Защита ускоренных соединений	H.235.6	7.6
8.6.1	Защита однонаправленного ускоренного соединения	H.235.6	7.6.1
8.6.1.1	Использование множественных алгоритмов шифрования в ускоренном соединении	H.235.6	7.6.1.1
8.6.2	Защита двухстороннего ускоренного старта	H.235.6	7.6.2
8.7	Зашифрованный DTMF-режим H.245	H.235.6	7.7
8.7.1	Зашифрованная основная строка	H.235.6	7.7.1
8.7.2	Зашифрованная строка iA5	H.235.6	7.7.2
8.7.3	Зашифрованная общая строка	H.235.6	7.7.3
8.7.4	Список идентификаторов объекта	H.235.6	7.7.4
8.8	Процесс Диффи-Хеллмана	H.235.6	7.8
9	Многоточечные процедуры	H.235.6	8.8
9.1	Аутентификация	H.235.6	8.8.1
9.2	Секретность	H.235.6	8.8.2
10	Сигнализация и процедуры аутентификации	H.235.0	8
10.1	Введение	H.235.0	---
10.2	Схема Диффи-Хеллмана с дополнительной аутентификацией	H.235.0	8.1
10.3	Аутентификация на основе подписи	H.235.0	8.2
10.3.1	Введение	H.235.0	–
10.3.2	Пароль с симметричным шифрованием	H.235.0	8.2.1
10.3.3	Пароль с хэшированием	H.235.0	8.2.2
10.3.4	Вариант, основанный на сертификатах с подписями	H.235.0	8.2.3
10.3.5	Использование общего секрета и паролей	H.235.0	8.2.4
11	Процедуры шифрования медиапотока	H.235.6	9
11.1	Сеансовые ключи медиа	H.235.6	9.1
11.2	Защита от рассылки спама медиа	H.235.6	9.2
11.2.1	Список идентификаторов объекта	H.235.6	9.2.1
12	Восстановление при ошибках защиты	H.235.0	11
13	Ассиметричная аутентификация и обмен ключами с использованием систем шифрования эллиптической кривой	H.235.0	9
13.1	Управление ключом	H.235.0	9.1

Таблица IV.1/H.235.0 – Соответствие пунктов

Пункт H.235v3Amd1Cor1	Название	Подсерия Рекомендаций H.235v4.x	Пункт
13.2	Цифровая подпись	H.235.0	9.2
Дополнение I	Подробности реализации H.323	H.235.0	Дополнение I
I.1	Метод дополнения шифротекста битами	H.235.6	I.1
I.2	Новые ключи	H.235.6	8.7.2
I.3	H.323 защитные элементы	H.235.6	8.7.3
I.4	Примеры реализации	H.235.0	I.1
I.4.1	Маркеры	H.235.0	I.1.1
I.4.2	Использование маркеров в системах H.323	H.235.0	I.1.2
I.4.3	Использование случайных значений H.235 в системах H.323	H.235.0	I.1.3
I.4.4	Пароль	H.235.0	I.1.4
I.4.5	IPsec	H.235.0	I.1.5
I.4.6	Поддержка серверных служб (BES)	H.235.0	I.1.6
Дополнение II	Подробности реализации H.324	H.235.0	Дополнение II
Дополнение III	Другие подробности реализации серии H	H.235.0	Дополнение III
Дополнение IV	Библиография	H.235.0	2.2
Приложение A	**ASN.1 H.235**	**H.235.0**	**Приложение A**
Приложение B	**Особые темы H.323**	**H.235.6**	**–**
B.1	Объяснение	H.235.0	6
B.2	Сигнализация и процедуры	H.235.6	8
B.2.1	Совместимость с редакцией 1	H.235.6	8.1
B.2.2	Сигнализация ошибок	H.235.0	11.1
B.2.3	Указание свойств версии 3	H.235.6	8.2
B.2.4	Передача ключа	H.235.6	8.3
B.2.4.1	Улучшенная передача ключа в H.235 версии 3	H.235.6	8.3.1
B.2.5	Улучшенный режим OFB	H.235.6	8.4
B.2.6	Обновление ключа и синхронизация	H.235.6	8.6
B.2.6.1	Неподтверждаемое обновление ключа	H.235.6	8.6.1
B.2.6.2	Улучшенное обновление ключа	H.235.6	8.6.2
B.2.6.3	Обновление и синхронизация ключа, основанные на типе полезной нагрузки	H.235.6	8.6.3
B.3	Формы RTP/RTCP	H.235.6	9.3
B.3.1	Вектор инициализации	H.235.6	9.3.1
B.3.1.1	Вектор инициализации CBC	H.235.6	9.3.1.1
B.3.1.2	Вектор инициализации EOFB	H.235.6	9.3.1.2
B.3.2	Дополнение битами	H.235.6	9.3.2
B.3.3	Защита RTCP	H.235.6	9.3.3

Таблица IV.1/H.235.0 – Соответствие пунктов

Пункт H.235v3Amd1Cor1	Название	Подсерия Рекомендаций H.235v4.x	Пункт
B.3.4	Защищенный поток полезной нагрузки	H.235.6	9.3.4
B.3.5	Взаимодействие с J.170	H.235.6	9.3.5
B.4	Сигнализация/процедуры RAS для аутентификации	H.235.0	8.3
B.4.1	Введение	H.235.0	–
B.4.2	Аутентификация конечная точка-привратник (не основанная на подписи)	H.235.0	8.3.1
B.4.3	Аутентификация конечная точка-привратник (основанная на подписи)	H.235.0	8.3.2
B.4.3.1	Пароль с симметричным шифрованием	H.235.0	8.3.2.1
B.4.3.2	Пароль с хэшированием	H.235.0	8.3.2.2
B.4.3.3	Вариант, основанный на сертификатах с подписями	H.235.0	8.3.3.3
B.5	Неоконечные взаимодействия	H.235.6	8.7
B.5.1	Шлюз	H.235.6	8.7.1
B.6	Управление ключом в канале RAS	H.235.0	8.4
B.7	Псевдослучайная функция (PRF)	H.235.0	10
Приложение C	**Вопросы специфики в H.324**	**H.235.0**	**Приложение B**
Приложение D	**Базовый профиль защиты**	**H.235.1**	
D.1	Введение	H.235.1	
D.2	Соглашения по терминам	H.235.1	5
D.3	Сфера применения	H.235.1	1
D.4	Сокращения	H.235.1	4
D.5	Нормативные справочные документы	H.235.1	2.1
D.6	Базовый профиль защиты	H.235.1	
D.6.1	Обзор	H.235.1	6.1
D.6.1.1	Применимость базового профиля защиты	H.235.1	6.2
D.6.1.2	Профиль защиты шифрования голоса	H.235.6	6.1
D.6.2	Аутентификация и целостность	H.235.1	3.1
D.6.3	Требования H.323	H.235.1	6.3
D.6.3.1	Обзор процедур	H.235.1	6.4
D.6.3.2	Аутентификация и целостность сообщений сигнализации на основе симметричного ключа (процедура I)	H.235.1	7
D.6.3.3	Вычисление хэша на основе пароля	H.235.1	7.1
D.6.3.3.1	HMAC-SHA1-96	H.235.1	7.2
D.6.3.3.2	Вычисление и проверка аутентификации и целостности	H.235.1	7.3
D.6.3.3.3	"Только аутентификация" (процедура IA)	H.235.1	8
D.6.3.4	Иллюстрация использования для процедуры I	H.235.1	9
D.6.3.4.1	Аутентификация и целостность сообщений RAS	H.235.1	9.1

Таблица IV.1/H.235.0 – Соответствие пунктов

Пункт H.235v3Amd1Cor1	Название	Подсерия Рекомендаций H.235v4.x	Пункт
D.6.3.4.2	Аутентификация и целостность сообщений H.225.0	H.235.1	9.2
D.6.3.4.3	Аутентификация и целостность сообщений H.245	H.235.1	9.3
D.6.4	Сценарий с прямой маршрутизацией	H.235.1	9.4
D.6.5	Поддержка серверных служб	H.235.1	10
D.6.6	Совместимость с H.235 версии 1	H.235.1	11
D.6.7	Многоадресный режим	H.235.1	12
D.7	Профиль защиты шифрования голоса	H.235.6	6.1
D.7.1	Управление ключом	H.235.6	8.5
D.7.2	Обновление ключа и синхронизация	H.235.6	8.6
D.7.3	Triple DES в режиме внешнего CBC	H.235.6	9.4
D.7.4	Алгоритм DES, работающий в режиме EOFB	H.235.6	9.5
D.7.5	Triple DES в режиме внешнего EOFB	H.235.6	9.6
D.8	Правомерное прослушивание	H.235.6	10
D.9	Список защищенных сообщений сигнализации	H.235.1	13
D.9.1	RAS H.225.0	H.235.1	13.1
D.9.2	Сигнализация вызова H.225.0	H.235.1	13.2
D.9.3	Контроль вызова H.245	H.235.1	13.3
D.10	Использование sendersID и generalID	H.235.1	14
D.11	Список идентификаторов объекта	H.235.1 H.235.6	15 11
D.12	Библиография	H.235.1 H.235.6	2.2 2.2
Приложение E	**Профиль защиты цифровой подписи**	**H.235.2**	
E.1	Общие положения	H.235.2	6
E.2	Соглашения по терминам	H.235.2	5
E.3	Требования H.323	H.235.2	6.1
E.4	Службы защиты	H.235.2	5
E.5	Цифровые подписи с элементами криптографической пары частный/открытый ключ (процедура II)	H.235.2	7
E.6	Процедуры многоточечных конференций	H.235.2	8
E.7	Сквозная аутентификация (процедура III)	H.235.2	9
E.8	Только аутентификация	H.235.2	10
E.9	Аутентификация и целостность	H.235.2	11
E.10	Вычисление цифровой подписи	H.235.2	12
E.11	Проверка цифровой подписи	H.235.2	13

Таблица IV.1/H.235.0 – Соответствие пунктов

Пункт H.235v3Amd1Cor1	Название	Подсерия Рекомендаций H.235v4.x	Пункт
E.12	Управление сертификатами	H.235.2	14
E.13	Пример использования процедуры II	H.235.2	15
E.13.1	Аутентификация, целостность и неотказуемость сообщений RAS	H.235.2	15.1
E.13.2	"Только аутентификация" RAS	H.235.2	15.2
E.13.3	Аутентификация, целостность и неотказуемость сообщений H.225.0	H.235.2	15.3
E.13.4	Аутентификация и целостность сообщений H.245	H.235.2	15.4
E.14	Совместимость с H.235 версии 1	H.235.2	16
E.15	Многоадресный режим	H.235.2	17
E.16	Список защищенных сообщений сигнализации	H.235.2	18
E.16.1	Сообщения H.225.0 RAS	H.235.2	18.1
E.16.2	Сообщения сигнализации вызова H.225.0	H.235.2	18.2
E.17	Использование sendersID и generalID	H.235.2	19
E.18	Список идентификаторов объекта	H.235.2	20
Дополнение IV (Приложение E)	Библиография	H.235.2	2.2
Приложение F	**Гибридный профиль защиты**	**H.235.3**	
F.1	Общие положения	H.235.3	6
F.2	Нормативные справочные документы	H.235.3	2.1
F.3	Сокращения	H.235.3	4
F.4	Соглашения по терминам	H.235.3	5
F.5	Требования H.323	H.235.3	6.1
F.6	Аутентификация и целостность	H.235.3	6.2
F.7	Процедура IV	H.235.3	7
F.8	Защищенное соединение для одновременных вызовов	H.235.3	8
F.9	Обновление ключа	H.235.3	9
F.10	Иллюстрирующие примеры	H.235.3	11
F.11	Многоадресный режим	H.235.3	12
F.12	Список защищенных сообщений сигнализации	H.235.3	13
F.12.1	Сообщения H.225.0 RAS	H.235.3	13.1
F.12.2	Сигнализация вызова (домен с одним администратором)	H.235.3	13.2
F.12.3	Сигнализация вызова H.225.0 (домен со многими администраторами)	H.235.3	13.3
F.13	Список идентификаторов объекта	H.235.3	14
Дополнение IV	Библиография	H.235.3	2.2

Таблица IV.1/H.235.0 – Соответствие пунктов

Пункт H.235v3Amd1Cor1	Название	Подсерия Рекомендаций H.235v4.x	Пункт
Приложение G	**Использование конфиденциального протокола передачи в режиме реального времени (SRTP) совместно с протоколом управления ключом MIKEY в H.235**	**H.235.7**	
G.1	Сфера применения	H.235.7	1
G.2	Справочные документы	H.235.7	2
G.2.1	Нормативные справочные документы	H.235.7	2.1
G.2.2	Информативные справочные документы	H.235.7	2.2
G.3	Термины и определения	H.235.7	3
G.4	Символы и сокращения	H.235.7	4
G.5	Соглашения по терминам	H.235.7	5
G.6	Введение	H.235.7	6
G.7	Общие положения и сценарии	H.235.7	7
G.7.1	Функционирование MIKEY на "сеансовом уровне"	H.235.7	7.1
G.7.2	Функционирование MIKEY на "уровне медиа"	H.235.7	7.2
G.7.3	Согласование возможностей MIKEY	H.235.7	7.3
G.8	Профиль защиты, использующий схему симметричного шифрования	H.235.7	8
G.8.1	Завершение вызова H.323	H.235.7	8.1
G.8.2	Смена ключей шифрования TGK и обновление CSB	H.235.7	8.2
G.8.3	Поддержка туннелирования H.245	H.235.7	8.3
G.8.4	Алгоритмы SRTP	H.235.7	8.4
G.8.5	Список идентификаторов объекта	H.235.7	8.5
G.9	Профиль защиты, использующий схему ассиметричного шифрования	H.235.7	9
G.9.1	Завершение вызова H.323	H.235.7	9.1
G.9.2	Смена ключа шифрования TGK и обновление CSB	H.235.7	9.2
G.9.3	Поддержка туннелирования H.245	H.235.7	9.3
G.9.4	Алгоритмы SRTP	H.235.7	9.4
G.9.5	Список идентификаторов объекта	H.235.7	9.5
G.I	Опция MIKEY-DHHMAC	H.235.7	Дополнение I
G.I.1	Завершение вызова H.323	H.235.7	I.1
G.I.2	Смена ключа шифрования TGK и обновление CSB	H.235.7	I.2
G.II	Использование Приложения I H.235 для создания предварительного общего секрета	H.235.7	Дополнение II
G.II.1	Завершение вызова H.323	H.235.7	II.1
G.II.2	Смена ключей шифрования TGK и обновление CSB	H.235.7	II.2

Таблица IV.1/H.235.0 – Соответствие пунктов

Пункт H.235v3Amd1Cor1	Название	Подсерия Рекомендаций H.235v4.x	Пункт
Приложение H	**Управление ключами RAS**	**H.235.5**	
H.1	Введение	H.235.5	–
H.2	Сфера применения	H.235.5	1
H.3	Справочные документы	H.235.5	2
H.3.1	Нормативные справочные документы	H.235.5	2.1
H.3.2	Информативные справочные документы	H.235.5	2.2
H.4	Определения	H.235.5	3
H.5	Сокращения по терминам	H.235.5	4
H.6	Основная структура	H.235.5	6
H.6.1	Улучшенные способности согласования в H.235.0	H.235.5	6.1
H.6.2	Использование между конечной точкой и привратником	H.235.5	6.2
H.6.3	Использование профиля между привратниками	H.235.5	6.3
H.6.4	Шифрование сигнализации канала и аутентификация	H.235.5	6.4
H.7	Специфический профиль защиты (SP1)	H.235.5	7
H.8	Расширения к структуре (информативно)	H.235.5	9
H.8.1	Использование главного ключа для сохранения канала сигнализации вызова через TLS	H.235.5	9.1
H.8.1.1	Регистрация конечной точки	H.235.5	9.1.1
H.8.2	Использование сертификатов для аутентификации привратника	H.235.5	9.2
H.8.3	Использование альтернативных механизмов защиты сигнализации	H.235.5	9.3
H.9	Угрозы (информативно)	H.235.5	10
H.9.1	Пассивная атака	H.235.5	10.1
H.9.2	Атаки "отказ от обслуживания"	H.235.5	10.2
H.9.3	Атаки через посредника	H.235.5	10.3
H.9.4	Предполагаемые атаки	H.235.5	10.4
H.9.5	Нешифрованная половина ключа привратника	H.235.5	10.5
Приложение I	**Поддержка вызовов прямой маршрутизации**	**H.235.4**	
I.1	Сфера применения	H.235.4	1
I.2	Введение	H.235.4	6
I.3	Соглашения по терминам	H.235.4	5
I.4	Термины и определения	H.235.4	3
I.5	Символы и сокращения	H.235.4	4
I.6	Нормативные справочные документы	H.235.4	2
I.7	Общие положения	H.235.4	7
I.8	Ограничения	H.235.4	8

Таблица IV.1/H.235.0 – Соответствие пунктов

Пункт H.235v3Amd1Cor1	Название	Подсерия Рекомендаций H.235v4.x	Пункт
I.9	Процедура DRC	H.235.4	9
I.10	Процедура получения ключа на основе PRF	H.235.4	12
I.11	Процедура получения ключа на основе FIPS-140	H.235.4	13
I.12	Список идентификаторов объекта	H.235.4	14
Дополнение I (Приложение I)	Библиография	H.235.4	2.2

Дополнение V

Соответствие рисунков H.235v3Amd1Cor1 подсерии Рекомендаций H.235v4

В этом информационном Дополнении приведено положение всех рисунков H.235v3Amd1Cor1 внутри подсерии Рекомендаций H.235v4.

Таблица V.1/H.235.0 – Соответствие рисунков

Рисунок H.235v3Amd1Cor1	Название	Подсерия Рекомендаций H.235v4.x	Рисунок
Рисунок 1	Схема Диффи-Хеллмана с дополнительной аутентификацией	H.235.0	4
Рисунок 2a	Пароль с симметричным шифрованием; два прохода	H.235.0	5
Рисунок 2b	Пароль с симметричным шифрованием; три прохода	H.235.0	6
Рисунок 3a	Пароль с хэшированием; два прохода	H.235.0	7
Рисунок 3b	Пароль с хэшированием; три прохода	H.230.0	8
Рисунок 4a	Вариант, основанный на сертификатах с подписями; два прохода	H.235.0	9
Рисунок 4b	Вариант, основанный на сертификатах с подписями; три прохода	H.235.0	10
Рисунок 5	Шифрование медиаданных	H.235.6	7
Рисунок 6	Дешифрование медиаданных	H.235.6	8
Рисунок 7	Формат пакета RTP для защиты от рассылки спама медиа	H.235.6	9
Рисунок I.1	Захват шифротекста в режиме ECB	H.235.6	I.1
Рисунок I.2	Захват шифротекста в режиме CBC	H.235.6	I.2
Рисунок I.2a	Дополнение нулевыми битами в режиме CBC	H.235.6	I.3
Рисунок I.3	Дополнение нулевыми битами в режиме CFB	H.235.6	I.4
Рисунок I.4	Дополнение нулевыми битами в режиме OFB	H.235.6	I.5
Рисунок I.4.1	Режим EOFB с дополнением нулевыми битами	H.235.6	I.6
Рисунок I.5	Дополнение битами, как предписано RTP	H.235.6	I.7

Таблица V.1/H.235.0 – Соответствие рисунков

Рисунок H.235v3Amd1Cor1	Название	Подсерия Рекомендаций H.235v4.x	Рисунок
Рисунок I.6	Маркеры	H.235.0	I.1
Рисунок I.7	Сценарий с сервером служб	H.235.0	I.2
Рисунок B.1	Общие положения	H.235.0	2
Рисунок B.1.1	Неподтверждаемое распознавание для распределения/обновления сеансового ключа от ведущего к ведомому(ым)	H.235.6	4
Рисунок B.1.2	Обновление сеансового ключа на логическом канале ведомого	H.235.6	5
Рисунок B.1.3	Обновление сеансового ключа на логическом канале ведущего	H.235.6	6
Рисунок B.2	Пароль с симметричным шифрованием	H.235.0	11
Рисунок B.3	Пароль с хэшированием	H.235.0	12
Рисунок B.4	Вариант, основанный на сертификатах с подписями	H.235.0	13
Рисунок D.1	Иллюстрация использования процедуры I в сценарии привратник-привратник с конечными точками, обеими находящимися в зонах с маршрутизацией привратником	H.235.1	1
Рисунок D.2	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	H.235.1	2
Рисунок D.3	Иллюстрация использования процедуры I в сценарии с конечными точками, обеими находящимися в зонах, в которых используется прямая маршрутизация привратником	H.235.1	3
Рисунок D.4	Шифрование Triple-DES в режиме внешнего CBC	H.235.6	10
Рисунок D.5	Шифрование Triple DES в режиме внешнего EOFB	H.235.6	11
Рисунок E.1	Одновременное использование защиты переход-за-переходом и сквозной аутентификации	H.235.2	1
Рисунок E.2	Иллюстрация использования открытого ключа в модели привратник-привратник	H.235.2	2
Рисунок F.1	Объединение методов защиты для параллельных вызовов	H.235.3	1
Рисунок F.2	Блок-схема в одиночном административном домене	H.235.3	2
Рисунок F.3	Блок-схема в множественном административном домене	H.235.3	3
Рисунок G.1	Сценарий	H.235.7	1
Рисунок G.2	Сценарий защиты с MIKEY и SRTP	H.235.7	2
Рисунок G.3	Сценарий переход-за-переходом только с общими секретами	H.235.7	3
Рисунок G.4	Конечная точка B примера вызывает конечную точку A (маршрутизация привратником) с предварительным общим MIKEY	H.235.7	4

Таблица V.1/H.235.0 – Соответствие рисунков

Рисунок H.235v3Amd1Cor1	Название	Подсерия Рекомендаций H.235v4.x	Рисунок
Рисунок G.5	Выполнение предварительного общего MIKEY конечной точкой B	H.235.7	5
Рисунок G.6	Выполнение предварительного общего MIKEY конечной точкой A	H.235.7	6
Рисунок G.7	Конечная точка B примера прекращает вызов	H.235.7	7
Рисунок G.8	Конечная точка B примера обновляет ключ	H.237.7	8
Рисунок G.9	Сценарий сквозного варианта с использованием PKI (множественные привратники)	H.235.7	9
Рисунок G.10	Конечная точка B примера вызывает конечную точку A (маршрутизация множественными привратниками) с помощью MIKEY-PK-SIGN	H.235.7	10
Рисунок G.11	Выполнение MIKEY-PK-SIGN конечной точкой B	H.235.7	11
Рисунок G.12	Выполнение MIKEY-PK-SIGN конечной точкой A	H.235.7	12
Рисунок G.13	Конечная точка B примера прекращает вызов	H.235.7	13
Рисунок G.14	Конечная точка B примера (инициатор) инициировала повторное снабжение ключами TGK и обновление ключей	H.235.7	14
Рисунок G.I-1	Конечная точка B примера вызывает конечную точку A (маршрутизация привратником) с помощью MIKEY-DHHMAC	H.235.7	I.1
Рисунок G.I-2	Конечная точка B примера прекращает вызов	H.235.7	I.2
Рисунок G.I-3	Конечная точка B примера обновляет ключ	H.235.7	I.3
Рисунок G.II-1	Конечная точка B примера вызывает конечную точку A (маршрутизация не привратником) с помощью предварительного общего MIKEY и DRC1 H.235.4	H.235.7	II.1
Рисунок H.1	Информационный поток для профиля защиты и TLS	H.235.5	1
Рисунок I.1	Сценарий вызова с прямой маршрутизацией	H.235.4	1
Рисунок I.2	Основной поток связи	H.235.4	2

Дополнение VI

Соответствие таблиц H.235v3Amd1Cor1 подсерии Рекомендаций H.235v4

В этом информационном Дополнении приведено положение всех таблиц H.235v3Amd1Cor1 внутри подсерии Рекомендаций H.235v4.

Таблица VI.1/H.235.0 – Соответствие таблиц

Таблица H.235v3Amd1Cor1	**Название**	**Подсерия Рекомендаций H.235v4.x**	**Таблица**
Таблица 1	Идентификатор объектов для NULL-шифрования	H.235.6	2
Таблица 2	Идентификаторы объектов для шифрования DTMF H.245	H.235.6	3
Таблица 3	Идентификаторы объектов, используемые для защиты от рассылки спама	H.235.6	5
Таблица I.1	Идентификаторы объектов, используемы в I.4.6	H.235.0	I.1
Таблица D.1	Сводка профилей защиты Приложения D	----	---
Таблица D.2	Базовый профиль защиты	H.235.1	1
Таблица D.3	Профиль шифрования голоса	H.235.6	1
Таблица D.4	Группы Диффи-Хеллмана	H.235.6	4
Таблица D.5	Использование sendersID и generalID	H.235.1	2
Таблица D.6	Идентификаторы объектов, используемые в Приложении D	H.235.1 H.235.6	3 6
Таблица E.1	Профиль защиты электронной подписи	H.235.2	1
Таблица E.2	Использование sendersID и generalID	H.235.2	2
Таблица E.3	Идентификаторы объектов, используемые в Приложении E	H.235.2	3
Таблица F.1	Обзор гибридного профиля защиты	H.235.3	1
Таблица F.2	Идентификаторы объектов, используемые в Приложении F	H.235.3	2
Таблица G.1	Протоколы управления ключом MIKEY	H.235.7	1
Таблица H.1	Элементы профиля	H.235.5	1
Таблица I.0	Вычисление шифрования и расширенных ключей из общего секрета	H.235.4	1
Таблица I.1	Идентификаторы объектов, используемые в H.235.4	H.235.4	2

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 защита
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.