МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

H.235.4

(09/2005)

СЕРИЯ H: АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

Инфраструктура аудиовизуальных услуг – Системные аспекты

Защита H.323: Защита вызовов с прямой и избирательной маршрутизацией

Рекомендация МСЭ-Т H.235.4

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.235.4

Защита H.323: Защита вызовов с прямой и избирательной маршрутизацией

Резюме

Целью данной Рекомендации является предоставление рекомендаций по обеспечению процедур защиты при использовании сигнализации вызова с прямой маршрутизацией в сочетании с профилями защиты H.235.1 и H.235.3. Данный профиль защиты является дополнительным и может быть дополнен профилями защиты Рек. МСЭ-Т H.235.1 и H.235.3. В профиле также приводятся детали реализации пункта 8.4/H.235.0 с помощью методик управления симметричным ключом.

В более ранних версиях подсерии H.235 этот профиль содержался в Приложении I/H.235. В Дополнениях IV, V, VI H.235.0 показано полное соответствие между пунктами, рисунками и таблицами версий 3 и 4 H.235.

Источник

Рекомендация МСЭ-Т H.235.4 утверждена 13 сентября 2005 года 16-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

Ключевые слова

Аутентификация, защита вызова с прямой маршрутизацией, шифрование, целостность, управление ключами, защита мультимедиа, профиль защиты, защита вызова с избирательной маршрутизацией.

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

Рекомендация МСЭ-Т H.235.4

Защита H.323: Защита вызовов с прямой и избирательной маршрутизацией

1 Сфера применения

Целью данной Рекомендации является предоставление рекомендаций по обеспечению процедур защиты при использовании сигнализации вызова с прямой и избирательной маршрутизацией в сочетании с профилями защиты H.235.1 и H.235.3.

Данный профиль защиты является дополнительным и может дополнять профили защиты H.235.1 или H.235.3. В профиле также приводятся детали реализации пункта 8.4/H.235.0 с помощью методик управления симметричным ключом.

2 Справочные документа

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, и стороны пришли к договоренности основываться на этой Рекомендации и стараться изыскивать 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*, Corrigendum 1 (2005), plus Erratum 1 (2005).

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

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

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

– 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.323 (2003), *Packet-based multimedia communications systems*.

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

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

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

2.2 Информативные справочные документы

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

– IETF RFC 4120 (2005), *The Kerberos Network Authentication Service (V5)*.

3 Термины и определения

В данной Рекомендации используются определения, данные в пункте 3 Рек. МСЭ-Т H.323, H.225.0, H.235.0 и X.800 | ИСО 7498-2.

4 Символы и сокращения

В этой Рекомендации используются следующие символы и сокращения:

CT	Маркер ClearToken
DH	Алгоритм Диффи-Хеллмана
DRC	Вызов с прямой маршрутизацией
EK_{AG}	Ключ шифрования, общий для EP A и GK G
EK_{BH}	Ключ шифрования, общий для EP B и GK H
EK_{GH}	Ключ шифрования, общий для GK G и GK H
$ENC_{K;\ S,\ IV}(M)$	Шифрование *M* EOFB с использованием секретного ключа *K*, секретного расширенного ключа *S* и вектора инициализации *IV*
EPID	Идентификатор конечной точки
GK	Привратник
GKID	Идентификатор привратника
g^x, g^y	Половина ключа Диффи-Хеллмана для GK G, GK H
K_{AB}	Ключ шифрования, общий для EP A и EP B
K_{AG}	Общий секрет (H.235.1, H.235.3) для EP A и GK G
K_{BH}	Общий секрет (H.235.1, H.235.3) для EP B и GK H
K_{GH}	Скрытый секрет (H.235.1, H.235.3) для GK G и GK H
KS_{AG}	Скрытый общий расширенный ключ для EP A и GK G
KS_{BH}	Скрытый общий расширенный ключ для EP B и GK H
KS_{GH}	Скрытый общий расширенный ключ для GK G и GK H
PRF	Псевдослучайная функция

5 Соглашения по терминам

В данной Рекомендации используются следующие соглашения:

– "должен" указывает на обязательное требование.

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

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

В тексте обращение к идентификаторам объектов происходит посредством символических ссылок (например, "I11"), в пункте 14 перечислены действительные числовые значения для символьных идентификаторов объектов, также см. пункт 5/H.235.0.

6 Введение

H.323 часто развертывается с использованием модели маршрутизируемого привратника (например, для повышения функциональности при учете времени). Широкое распространение моделей вызова с

маршрутизируемым привратником также является причиной, по которой в различных профилях защиты внимание акцентировано исключительно на данной модели вызова, Рек. МСЭ-Т H.235.0 (такие как H.235.1, H.235.2, H.235.3).

Однако, по мере необходимости поддержки увеличивающегося количества параллельных каналов, модель с прямой маршрутизацией вызова с привратником может дать лучшие результаты для таких характеристик, как производительность и масштабируемость. Преимуществом данного режима является использование привратника для регистрации, допуска, разрешения адреса и контроля полосы пропускания, во время выполнения установления вызова непосредственно между конечными точками в сквозной форме.

В данной Рекомендации описывается расширение возможностей базового H.235.1 и смешанного H.235.3 профилей защиты для поддержки прямой маршрутизации вызовов с привратником(ами).

7 Общие положения

Базовый профиль защиты H.235.1, так же как и гибридный H.235.3, используют общий секрет (после первого квитирования), чтобы убедиться, что сообщение аутентификации и/или целостность для формы переход-переход используют привратника в качестве доверенного промежуточного устройства. При использовании модели прямой маршрутизации вызова не может использоваться общий секрет для двух конечных точек. Также в практическом применении не используется для защиты связи предварительно установленный общий секрет, так как в данном случае всем конечным точкам будет предварительно известно, какая другая конечная точка будет вызвана.

Рек. МСЭ-Т H.235.4 обращается к сценарию, показанному на рисунке 1, где конечные точки соединены с привратником и развернута сигнализация с прямой маршрутизацией вызова. В сценарии предполагается использование незащищенной IP-сети в области привратника.

Предполагается, что каждая конечная точка имеет относительную связь и защищенное соединение с ее привратником, и каждая конечная точка была надежно зарегистрирована привратником с помощью базового или смешанного профиля защиты.

Поэтому привратник инициирующей конечной точки (DRC1) или привратник завершающей конечной точки (DRC2) могут предоставить общий секрет для сообщающихся напрямую конечных точек, используя подход, подобный Kerberos (см. RFC 4120).

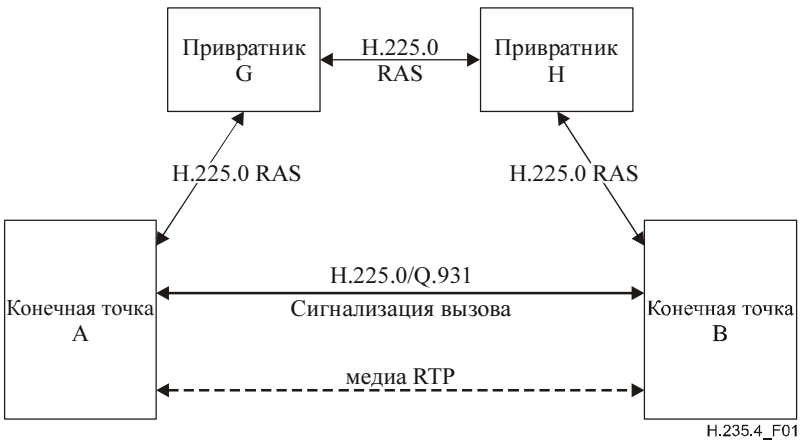

Рисунок 1/H.235.4 – Сценарий с прямой маршрутизацией вызова

В данной Рекомендации отображены две процедуры для различного окружения – DRC1 и DRC2.

Процедура DRC1 (см. пункт 9) применяется в корпоративной среде, где привратники расположены в пределах различных (локальных) местоположений, но местоположения придерживаются общей корпоративной политики защиты. В такой среде является допустимым определение эффективной политики защиты для установления вызова вызывающим привратником G, соответственно

вызывающим привратником G выбираются применяемые параметры защиты. Завершающим привратником H будут приняты выбранные параметры защиты.

Процедуры DRC2 (см. пункт 10) и DRC3 (пункт 11) могут применяться в междоменных средах, где привратники расположены в пределах различных административных доменов и каждый домен может использовать различную политику защиты.

Процедура DRC2 может применяться в случаях, когда вызывающая конечная точка или привратник не поддерживают алгоритм Диффи-Хеллмана. В такой среде является допустимым определение эффективной политики защиты для установления вызова завершающим привратником H, соответственно завершающим привратником H выбираются применяемые параметры защиты. Вызывающим привратником G будут приняты выбранные параметры защиты.

Процедура DRC3 может применяться в случаях, когда вызывающей конечной точкой не поддерживается алгоритм Диффи-Хеллмана, в то время как обоими привратниками в вызывающем и вызываемом доменах алгоритм Диффи-Хеллмана поддерживается.

В начале регистрации вызова процедуры выполняют обмен сигналами, чтобы согласовать, которая из процедур DRC1, DRC2 или DRC3 будет применена.

8 Ограничения

Данная Рекомендация не предназначена для сценариев с прямой маршрутизацией без участия какого-либо привратника. Эта тема остается на будущее изучение.

9 Процедура DRC1 (корпоративная среда)

Процедура, описанная в этом пункте, применяется в корпоративной среде, где привратники расположены в пределах различных (локальных) местоположений, но местоположения придерживаются общей корпоративной политики защиты. В такой среде является допустимым определение эффективной политики защиты для установления вызова вызывающим привратником G, соответственно вызывающим привратником выбираются применяемые параметры защиты. Завершающим привратником H будут приняты выбранные параметры защиты.

9.1 Фаза GRQ/RRQ

Конечными точками, способными поддерживать данный профиль защиты, эта возможность должна быть указана во время фазы **GRQ** и/или **RRQ**, включением отдельного ClearToken с присвоенным значением "I10" полю **tokenOID**, любые другие поля в данном ClearToken не должны использоваться. Совместимый с H.235.4 привратник, готовый обеспечить необходимые функциональные возможности, должен ответить сообщением **GCF** или **RCF** с отдельным ClearToken, включающим поле **tokenOID** с присвоенным значением "I10", все другие поля в ClearToken не должны использоваться.

9.2 Фаза ARQ

Перед тем как конечная точка A начнет отправку сообщений сигнализации вызова напрямую к другой конечной точке B, конечная точка A или B должна обратиться с запросом на допуск к привратнику G или H, используя сообщение **ARQ**. Конечная точка A должна включить в сообщение **ARQ** отдельный ClearToken с присвоенным значением "I10" полю **tokenOID**, все другие поля в ClearToken не должны использоваться.

9.3 Фаза LRQ

В данной процедуре рассмотрены случаи применения как одиночного общего для конечных точек привратника, так и нескольких привратников выстроенных в цепочку. При применении схемы с несколькими привратниками привратник G, в зоне которого инициируется вызов, должен обнаружить привратника H с помощью широковещательного механизма **LRQ**, как описывается в Рек. МСЭ-Т H.323, пункт 8.1.6, "Сигнализация произвольно вызываемой конечной точки". Связь между двумя привратниками должна быть защищена в соответствии с H.235.1. Предполагается, что для этого доступен общий секрет K_{GH}. Так как сообщение **LRQ** передаваемое между привратниками обычно является широковещательным сообщением, общий секрет K_{GH}, как правило, не может быть

двухточечным общим секретом, но предполагается, что фактически это будет групповой общий секрет в пределах множества возможных привратников.

ПРИМЕЧАНИЕ. – Это накладывает ограничения масштабируемости в общих случаях применения и не позволяет выполнить аутентификацию источника. Однако предполагается, что в корпоративных сетях с ограниченным, небольшим количеством общеизвестных привратников такое ограничение и ограничения защиты являются приемлемыми. Защита широковещательной связи между привратниками с помощью цифровых подписей может компенсировать данные ограничения: однако эта тема остается на будущее изучение.

Если **LRQ** механизм используется, чтобы обнаружить привратник, расположенный в удаленном конце сети, сообщением **LRQ** должен быть передан отдельный маркер ClearToken с присвоенным значением "I10" полю **tokenOID**; любые другие поля в данном маркере ClearToken не должны использоваться. При отправке широковещательного сообщения **LRQ** в маркере ClearToken поле **generalID** не должно использоваться. Тема связи между привратниками с использованием H.501 и/или H.510 оставлена на будущее изучение.

9.4 Фаза LCF

EK_{BH} обозначает ключ шифрования, KS_{BH} обозначает расширенный ключ, общий для конечной точки B и привратника H. Как описано ниже, привратник H и конечная точка B по отдельности вычисляют материал ключа из общего секрета K_{BH}, используя функцию PRF.

Привратником H должны быть сгенерированы: случайный Challenge-B, материал ключа шифрования EK_{BH} и материал расширенного ключа KS_{BH} из общего секрета K_{BH} с помощью процедуры выведения ключа на основе PRF, как описано в пункте 12, в котором Challenge-B заменено на **challenge** и CT_{HG}**→h235Key→secureSharedSecret→keyDerivationOID** должно содержать "AnnexI-HMAC-SHA1-PRF", см. пункт 14.

EK_{GH} обозначает ключ шифрования, KS_{GH} обозначает расширенный ключ, который является общим для привратника G и привратника H. Привратником H должно быть сгенерировано одно случайное сообщение Challenge-G. Привратником H должны быть сгенерированы материал ключа шифрования EK_{GH} и материал расширенного ключа KS_{GH} из общего секрета K_{GH} с помощью процедуры выведения ключа PRF, как описано в пункте 14, в котором Challenge-G заменено на **challenge**. CT_{HG}**→challenge** должен содержать Challenge-G, для CT_{HG}**→h235Key→secureSharedSecret→generalID** должен быть присвоен идентификатор конечной точки B.

Привратник H должен передать зашифрованные ключи EK_{BH} и KS_{BH} привратнику G. Также должен использоваться расширенный режим шифрования OFB (EOFB) (см. 8.4/H.235.6) с секретным расширенным ключом конечной точки KS_{GH}. Алгоритмы шифрования, которые могут быть применены (см. таблицу 6/H.235.6):

– DES (56 битов) в режиме EOFB, используя OID "Y1": по усмотрению;

– 3DES (168 битов) в режиме внешнего EOFB, используя OID "Z1": по усмотрению;

– AES (128 битов) в режиме EOFB, используя OID "Z2": рекомендуется и является установленным по умолчанию;

– RC2-совместимый (56 битов) в режиме EOFB, используя OID "X1": по усмотрению.

Для режима шифрования EOFB привратником H должно быть сгенерировано случайное начальное значение IV. Для OID "X1", OID "Y1" и OID "Z1" значение IV имеет длину 64 бита и должно быть передано в CT_{HG}**→h235Key→secureSharedSecret→params→iv8**; поскольку значение IV для OID "Z2" имеет длину 128 битов, оно должно быть передано в CT_{HG}**→h235Key→secureSharedSecret→params→iv16**.

Привратником H должно быть включено $ENC_{EKGH,\ KSGH,\ IV}(EK_{BH})$ и $ENC_{EKGH,\ KSGH,\ IV}(KS_{BH})$ в ClearToken CT_{HG} с присвоенным значением "I13" в поле **tokenOID**. Полученное зашифрованное сообщение $ENC_{EKGH,\ KSGH,\ IV}(EK_{BH})$ должно быть передано в CT_{HG}**→h235Key→secureSharedSecret→encryptedSessionKey**; полученное зашифрованное сообщение $ENC_{EKGH,\ KSGH,\ IV}(KS_{BH})$ должно быть передано в CT_{HG}**→h235Key→secureSharedSecret→encryptedSaltingKey**. Алгоритм шифрования должен быть указан в CT_{HG}**→h235Key→algorithmOID** ("X1", "Y1", "Z1" или "Z2"). Challenge-B должен быть помещен в CT_{HG}**→h235Key→secureSharedSecret→clearSaltingKey**. CT_{HG}**→generalID** должно быть присвоено значение идентификатора привратника G, тогда как CT_{HG}**→sendersID** должно быть присвоено значение идентификатора привратника H.

Challenge-B должен быть передан в конечную точку B путем включения элемента **profileInfo** в **ClearToken** – CT_{HG}→**profileInfo→elementID** = 0 определяет данный элемент профиля;

CT_{HG}→**profileInfo→paramS** должно остаться неиспользованным, а CT_{HG}→**profileInfo→element→octets** должно содержать Challenge-B.

В ответном сообщении **LCF** должен содержаться ClearToken CT_{HG}.

9.5 Фаза ACF

Если привратник G распознал наличие поддержки данной Рекомендации конечными точками A и B, им должны быть сгенерированы материал ключа и ClearTokens, как описано ниже.

Кроме обычной операции **ARQ** привратником может быть вычислен общий секрет K_{AB} на основе вызова. Этот общий секрет на основе вызова затем будет распространен с помощью ClearTokens между обеими конечными точками. Данные ClearTokens должны быть переданы в сообщении **ACF** и отправлены обратно вызывающему устройству.

Оба ClearTokens должны содержать первый CT_A для вызывающего устройства A и другой CT_B для вызываемого устройства B. В каждом **ClearToken** в **tokenOID** должно содержаться значение OID ("I11" или "I12"), которое указывает, предназначен ли маркер для вызывающего устройства (OID "I11" для CT_A) или для вызываемого устройства (OID "I12" для CT_B).

GK G должен расшифровать CT_{HG}→**h235Key→secureSharedSecret→encryptedSessionKey** чтобы получить $EK_{BH,}$ затем расшифровать CT_{HG}→**h235Key→secureSharedSecret→encryptedSaltingKey** чтобы получить KS_{BH}.

Как описано в данной Рекомендации, **ClearToken** может использоваться в сочетании с другими профилями защиты, например H.235.1 или H.235.3 в которых также описано развертывание ClearTokens. В таком случае в ClearToken описанном в данной Рекомендации должны использоваться также другие поля **ClearToken**. Например, при использовании этой Рекомендации в сочетании с Рек. МСЭ-Т H.235.1 должны быть представлены и использованы поля **timestamp**, **random**, **generalID**, **sendersID**, и **dhkey**, как описано в профиле защиты H.235.1.

Идентификатор привратника (GKID) G должен быть помещен в CT_A→**sendersID** и CT_B→**sendersID**, тогда как CT_A→**generalID** должен содержать идентификатор конечной точки A и CT_B→**generalID** идентификатор конечной точки B.

Привратником G должны быть сгенерированы из K_{GH} материал расширенного ключа KS_{GH} и материал ключа шифрования EK_{GH}, с помощью процедуры выведения ключа на основе PRF, как описано в пункте 12, где **challenge** необходимо заменить CT_{HG}→**challenge**.

Ключи шифрования EK_{AG} и EK_{BH} для зашифрованного сквозного ключа K_{AB} должны быть выведены из общего секрета между привратником и конечными точками (EK_{AG} или EK_{BH}), используя процедуру выведения ключа на основе PRF, как описано в пункте 12, где CT_A→**h235Key→secureSharedSecret→keyDerivationOID** и CT_B→**h235Key→secureSharedSecret→keyDerivationOID** должны содержать "AnnexI-HMAC-SHA1-PRF", см. пункт 14, а также CT_A→**challenge** должен содержать Challenge-A.

Привратником G Challenge-B должен быть скопирован из CT_{HG}→**h235Key→secureSharedSecret→clearSaltingKey** в CT_B→**challenge**.

Поле CT_B→**profileInfo** должно содержать элемент профиля, который был передан в CT_{HG} **profileInfo** при условии, что в конце конечная точка B получит Challenge-B.

Данный секрет сеанса K_{AB} должен быть зашифрован с помощью EK_{AG} (для CT предназначенного для конечной точки A) или EK_{BH} (для CT предназначенного для конечной точки B), используя алгоритм шифрования.

Должен использоваться расширенный режим шифрования OFB (EOFB) (см. 8.4/H.235.6) с секретным расширенным ключом конечной точки KS_{AG} или KS_{BH}. Алгоритмы шифрования, которые могут быть применены (см. таблицу 6/H.235.6):

– DES (56 битов) в режиме EOFB, используя OID "Y1": по усмотрению;

– 3DES (168 битов) в режиме внешнего EOFB, используя OID "Z1": по усмотрению;

– AES (128 битов) в режиме EOFB, используя OID "Z2": рекомендуется и является установленным по умолчанию;

– RC2-совместимый (56 битов) в режиме EOFB, используя OID "X1": по усмотрению.

Для режима шифрования EOFB привратником G должно быть сгенерировано случайное начальное значение IV. Для OID "X1", OID "Y1" и OID "Z1" значение IV имеет длину 64 бита и должно быть передано в CT_A→**h235Key→secureSharedSecret→params→iv8** и в CT_B→**h235Key→secureSharedSecret→params→iv8**; поскольку значение IV для OID "Z2" имеет длину 128 битов, оно должно быть передано в CT_A→**h235Key→secureSharedSecret→params→iv16** и в CT_B→**h235Key→secureSharedSecret→params→iv16**.

Полученное зашифрованное сообщение $ENC_{EKAG,\ KSAG,\ IV}(K_{AB})$ должно быть передано в CT_A→**h235Key→secureSharedSecret→encryptedSessionKey**, а зашифрованное сообщение $ENC_{EKBH,\ KSBH,\ IV}(K_{AB})$ должно быть передано в CT_B→**h235Key→secureSharedSecret→encryptedSessionKey**. Алгоритм шифрования должен быть указан в CT_A→**h235Key→secureSharedSecret→algorithmOID** и в CT_B→**h235Key→secureSharedSecret→algorithmOID** – ("X1", "Y1", "Z1" или "Z2").

Для маркера ClearToken, предназначенного для конечной точки A, в CT_A→**h235Key→secureSharedSecret→generalID** должен быть помещен идентификатор конечной точки B ($EPID_B$). Точно также для маркера ClearToken, предназначенного для конечной точки B, в CT_B→**h235Key→secureSharedSecret→generalID** должен быть помещен идентификатор конечной точки A ($EPID_A$).

Для алгоритмов шифрования EOFB поле **encryptedSaltingKey** не должно использоваться.

Привратником G должны быть включены оба маркера ClearTokens CT_A и CT_B в сообщение **ACF**, которое отправляется по направлению к конечной точке A.

9.6 Фаза SETUP

Конечной точкой A должен быть распознан маркер CT_A путем проверки в ClearToken поля **tokenOID**, которое должно иметь значение "I11".

Конечная точка A должна выполнить проверку на давность полученного маркера CT_A с помощью проверки поля **timestamp**. Дальнейшие проверки защиты должны проверять **generalID** и **sendersID** в ClearToken и **generalID** в **V3KeySyncMaterial**. Если полученный маркер CT_A прошел проверку на давность, конечная точка A должна извлечь IV и вычислить EK_{AG} и KS_{AG} для привратника G, как описано выше. Чтобы получить $K_{AB,}$ конечной точкой A должны быть расшифрованы сведения **encryptedSessionKey**, используемые в поле **secureSharedSecret** маркера CT_A.

Если полученный маркер CT_A прошел проверку на давность, конечная точка A сможет отправить сообщение SETUP конечной точке B. Данное сообщение SETUP включает маркер CT_B. Сообщение SETUP должно быть защищено (аутентификацией и/или защищенной целостностью) в соответствии с Рек. МСЭ-Т H.235.1 или Рек. МСЭ-Т H.235.3, используя ключ K_{AB} в качестве применяемого общего секрета. Для этого поле **generalID** в хешированном, в соответствии с H.235.1, маркере ClearToken (не CT_B!) не должно быть использованным, за исключением случаев, когда конечная точка A уже имеет значение $EPID_B$ (например, через конфигурацию или сохраненное в памяти с предыдущего соединения). Если конечной точкой A используется значение $EPID_B$ в поле generalID сообщения SETUP, тогда значение sendersID в возвращенном сообщении сигнализации вызова должно быть принято конечной точкой A как истинное значение $EPID_B$.

Конечной точкой B должен быть распознан маркер CT_B путем проверки в ClearToken поля **tokenOID**, которое должно иметь значение "I12".

Конечная точка B должна выполнить проверку на давность полученного маркера CT_B с помощью проверки поля **timestamp**. Дальнейшие проверки защиты должны проверять **sendersID** в ClearToken и **generalID** в **secureSharedSecret**. Если полученный маркер CT_B прошел проверку на давность, конечной точкой B из CT_{HG}→**profileInfo→element→octets** должен быть извлечен Challenge-B, также необходимо извлечь IV и вычислить EK_{BH} и KS_{BH}, в пункте 12 Challenge-B заменено на **challenge**, как упоминалось выше для привратника. Чтобы получить $K_{AB,}$ конечной точкой B должны быть расшифрованы сведения **encryptedSessionKey**, используемые в поле **secureSharedSecret** маркера CT_B.

В случае если маркер CT_B прошел проверку на давность, конечной точкой B может быть продолжена сигнализация вызова путем отправки команд CALL-PROCEEDING, ALERTING или CONNECT и т. д. В случае если маркер CT_B не прошел проверку на давность или проверка защиты в сообщении

SETUP была не выполнена, конечная точка B должна ответить командой RELEASE-COMPLETE и полю **ReleaseCompleteReason** присвоить значение ошибки защиты, как определено в пункте 11.1/H.235.0.

Если защита среды развернута (см. 6.1/H.235.6), конечные точки A и B должны обменяться половинами ключей Диффи-Хеллмана в соответствии с 8.5/H.235.6 и создать динамический сеансовый ведущий ключ, из которого затем могут быть получены сеансовые ключи среды.

Конечная точка должна включать в сообщения поле **generalID** с присвоенным значением $EPID_A$ и поле **sendersID** с присвоенным значением $EPID_B$ для защиты любых H.225.0 сообщений сигнализации вызова предназначенных для EP A (например, Call Proceeding, Alerting или Connect).

На рисунке 2 показан базовый процесс связи:

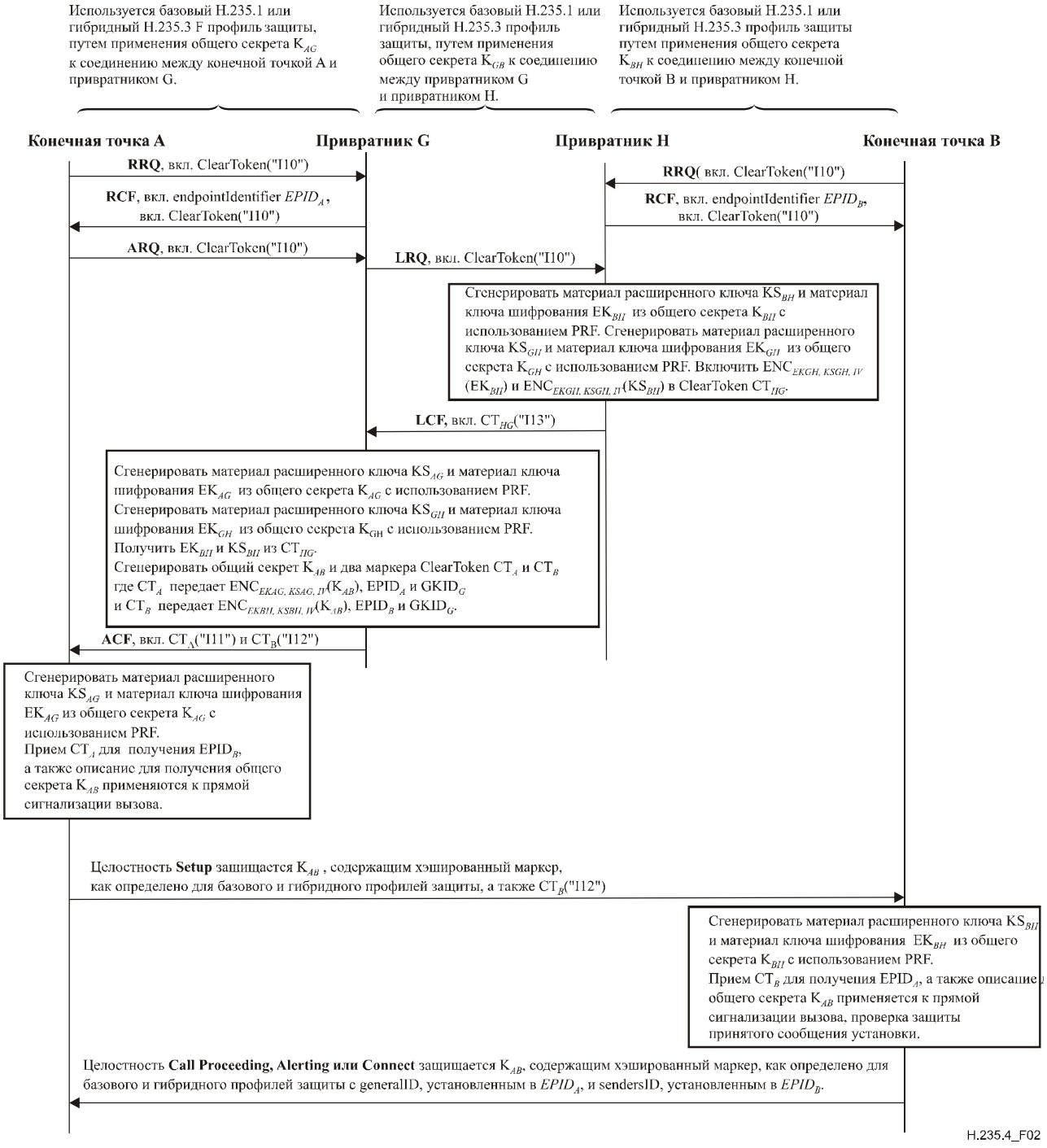

Рисунок 2/H.235.4 – Базовый процесс связи (DRC1)

10 Процедура DRC2 (междоменная среда)

Процедура, описанная в этом пункте, может применяться в междоменных средах, в которых привратники расположены в пределах различных административных доменов и каждый домен может использовать различную политику защиты. Процедура DRC2 может применяться в случаях, когда вызывающая конечная точка или привратник не поддерживают алгоритм Диффи-Хеллмана.

В такой среде является допустимым определение эффективной политики защиты для установления вызова завершающим привратником H; соответственно завершающим привратником H выбираются применяемые параметры защиты. Вызывающим привратником G будут приняты выбранные параметры защиты.

10.1 Фаза GRQ/RRQ

Конечными точками, способными поддерживать данный профиль защиты, эта способность должна быть указана во время фазы **GRQ** и/или **RRQ**, включением отдельного маркера ClearToken с присвоенным значением "I20" полю **tokenOID**, любые другие поля в данном маркере ClearToken не должны использоваться. Совместимый с H.235.4 привратник, готовый обеспечить необходимые функциональные возможности, должен ответить сообщением **GCF** или **RCF** с отдельным маркером ClearToken, включающим поле **tokenOID** с присвоенным значением "I20", все другие поля в маркере ClearToken не должны использоваться.

10.2 Фаза ARQ

Перед тем как конечная точка A начнет отправку сообщений сигнализации вызова напрямую к другой конечной точке B, конечная точка A или B должна обратиться с запросом на допуск к привратнику G или H, используя сообщение **ARQ**. Конечная точка A должна включить в сообщение **ARQ** отдельный маркер ClearToken с присвоенным значением "I20" полю **tokenOID**, все другие поля в маркере ClearToken не должны использоваться.

10.3 Фаза LRQ

В данной процедуре рассмотрены случаи применения как одиночного общего для конечных точек привратника, так и нескольких привратников выстроенных в цепочку. При применении схемы с несколькими привратниками привратник G, в зоне которого инициируется вызов, должен обнаружить привратника H с помощью широковещательного механизма **LRQ**,как описывается в Рек. МСЭ-Т H.323, пункт 8.1.6, "Сигнализация произвольно вызываемой конечной точки". Связь между двумя привратниками должна быть защищена в соответствии с Рек. МСЭ-Т H.235.1. Предполагается, что для этого доступен общий секрет $K_{GH.}$ Так как сообщение **LRQ** передаваемое между привратниками обычно является широковещательным сообщением, общий секрет $K_{GH,}$ как правило, не может быть двухточечным общим секретом, но предполагается, что фактически это будет групповой общий секрет в пределах области возможных привратников.

ПРИМЕЧАНИЕ. – Это накладывает ограничения масштабируемости в общих случаях применения и не позволяет выполнить аутентификацию источника. Однако полагается, что в корпоративных сетях с ограниченным, небольшим количеством общеизвестных привратников такое ограничение и ограничения защиты являются приемлемыми. Защита широковещательной связи между привратниками с помощью цифровых подписей может компенсировать данные ограничения: однако эта тема остается на будущее изучение.

Если **LRQ** механизм используется, чтобы обнаружить привратник, расположенный в удаленном конце сети, сообщением **LRQ** должен быть передан отдельный маркер ClearToken с присвоенным значением "I20" полю **tokenOID**; любые другие поля в данном маркере ClearToken не должны использоваться. При отправке широковещательного сообщения **LRQ** в маркере ClearToken поле **generalID** не должно использоваться. Тема связи между привратниками с использованием H.501 и/или H.510 оставлена на будущее изучение.

10.4 Фаза LCF

Если привратник H распознал наличие поддержки данной Рекомендации конечными точками A и B, им должен быть сгенерирован материал ключа и маркеры ClearToken в **LCF** , как описано ниже.

K_{BH} обозначает общий секрет, который является общим для конечной точки B и привратника H. EK_{BH} обозначает ключ шифрования, KS_{BH} обозначает расширенный ключ, общий для конечной точки B и привратника H. Привратником H должен быть сгенерирован один случайный Challenge-B. Привратником H должны быть сгенерированы материал ключа шифрования EK_{BH} из общего секрета

K_{BH} с помощью процедуры выведения ключа на основе PRF, как определено в пункте 12, в котором Challenge-B заменено на **challenge** и CT_B→**h235Key→secureSharedSecret→keyDerivationOID** должно содержать "AnnexI-HMAC-SHA1-PRF", см. пункт 14.

Привратником H должен быть сгенерирован расширенный ключ KS_{BH} из ключа K_{BH} с помощью процедуры выведения ключа на основе PRF, как определено в пункте 12, где Challenge-B нужно заменить на **challenge**.

EK_{GH} обозначает ключ шифрования, KS_{GH} обозначает расширенный ключ, общий для привратника G и привратника H. Привратником H должен быть сгенерирован один случайный Challenge-G. Привратником H должны быть сгенерированы материал ключа шифрования EK_{GH} из общего секрета K_{GH} с помощью процедуры выведения ключа на основе PRF, как определено в пункте 12, в котором Challenge-G заменено на **challenge** и CT_{HG}→**h235Key→secureSharedSecret→keyDerivationOID** должно содержать "AnnexI-HMAC-SHA1-PRF", см. пункт 14.

Привратником H должен быть сгенерирован ключ KS_{GH} из общего секрета K_{GH} с помощью процедуры выведения ключа на основе PRF, как определено в пункте 12, где Challenge-G нужно заменить на **challenge**.

Привратником H создаются два маркера ClearTokens в сообщении **LCF**. Один маркер CT_{HG} для привратника G и маркер CT_B для вызываемого устройства B. CT_{HG}→**tokenOID** должно содержать OID с присвоенным значением "I23" тогда как CT_B→**tokenOID** должно содержать OID с присвоенным значением "I12".

Challenge-G должен быть присвоен полю CT_{HG}→**challenge**, идентификатор привратника H должен быть присвоен CT_{HG}→**sendersID**, идентификатор привратника G (скопированный из сообщения **LRQ**) должен быть присвоен CT_{HG}→**generalID**.

Challenge-B должен быть присвоен полю CT_B→**challenge**, идентификатор привратника H должен быть присвоен CT_B→**sendersID**, идентификатор конечной точки B должен быть присвоен CT_B→**generalID**. Если в сообщении **LRQ** имеется идентификатор конечной точки A в поле endpointIdentifier, привратником H данный идентификатор должен быть скопирован в CT_B→**h235Key→secureSharedSecret→generalID**, а также в CT_{HG}→**h235Key→secureSharedSecret→generalID**.

Если привратник H и конечная точка B поддерживают процедуру DRC2 данной Рекомендации, ответное сообщение **LCF** должно содержать маркеры ClearToken CT_{HG} и CT_B.

Привратник G, получивший сообщение **LCF** от привратника H, проверит маркеры ClearToken CT_B и CT_{HG}. Привратником G используются Challenge-G вместо **challenge** и функция PRF, как описано в пункте 12 для вычисления ключей KS_{GH} и EK_{GH} из ключа K_{GH}, а затем для расшифровки CT_{HG}→**h235Key→secureSharedSecret→encryptedSessionKey** и получения ключа K_{AB}, общего для конечных точек A и B.

10.5 Фаза ACF

Привратником H на основе вызова вычисляется общий секрет K_{AB}, общий для конечных точек A и B. Этот общий секрет на основе вызова затем будет распространен с помощью маркеров ClearTokens между обеими конечными точками. Маркер ClearToken сначала отправляется обратно вызывающему привратнику G, затем привратник G передает сведения сообщением **ACF** обратно вызывающему устройству.

Привратник H должен зашифровать ключ K_{AB} с помощью EK_{GH}, как $ENC_{EKHG,\ KSHG,\ IV}(K_{AB})$ и поместить зашифрованный ключ K_{AB} в CT_{HG}→**h235Key→secureSharedSecret→encryptedSessionKey**.

Должен использоваться расширенный режим шифрования OFB (EOFB) (см. 8.4/H.235.6) с секретным расширенным ключом конечной точки KS_{GH}. Алгоритмы шифрования, которые могут быть применены (см. таблицу 6/H.235.6):

– DES (56 битов) в режиме EOFB, используя OID "Y1": по усмотрению;

– 3DES (168 битов) в режиме внешнего EOFB, используя OID "Z1": по усмотрению;

– AES (128 битов) в режиме EOFB, используя OID "Z2": рекомендуется и является установленным по умолчанию;

– RC2-совместимый (56 битов) в режиме EOFB, используя OID "X1": по усмотрению.

Для режима шифрования EOFB привратником H должно быть сгенерировано случайное начальное значение IV. Для OID "X1", OID "Y1" и OID "Z1" значение IV имеет длину 64 бита и должно быть передано в CT_{HG}→**h235Key→secureSharedSecret→params→iv8**; поскольку значение IV для OID "Z2" имеет длину 128 битов, оно должно быть передано в CT_{HG}→**h235Key→secureSharedSecret→params→iv16**.

Алгоритм шифрования должен быть указан в CT_{HG}→**h235Key→secureSharedSecret→algorithmOID** ("X1", "Y1", "Z1" или "Z2"). Для алгоритмов шифрования EOFB поле **encryptedSaltingKey** не должно использоваться.

Подобным образом привратник H должен зашифровать ключ K_{AB} с помощью EK_{BH}, как $ENC_{EKBH, KSBH, IV}(K_{AB})$ и поместить зашифрованный ключ K_{AB} в CT_B→**h235Key→secureSharedSecret→encryptedSessionKey**.

Должен использоваться расширенный режим шифрования OFB (EOFB) (см. 8.4/H.235.6) с секретным расширенным ключом конечной точки KS_{BH} для конечной точки B (CT_B). Алгоритмы шифрования, которые могут быть применены (см. таблицу 6/H.235.6):

– DES (56 битов) в режиме EOFB, используя OID "Y1": по усмотрению;

– 3DES (168 битов) в режиме внешнего EOFB, используя OID "Z1": по усмотрению;

– AES (128 битов) в режиме EOFB, используя OID "Z2": рекомендуется и является установленным по умолчанию;

– RC2-совместимый (56 битов) в режиме EOFB, используя OID "X1": по усмотрению.

Для режима шифрования EOFB привратником H должно быть сгенерировано случайное начальное значение IV. Для OID "X1", OID "Y1" и OID "Z1" значение IV имеет длину 64 бита и должно быть передано в CT_B→**h235Key→secureSharedSecret→ params→iv8**; поскольку значение IV для OID "Z2" имеет длину 128 битов, оно должно быть передано в CT_B→**h235Key→secureSharedSecret→params→iv16**.

Алгоритм шифрования должен быть указан в CT_B→**h235Key→secureSharedSecret→algorithmOID** ("X1", "Y1", "Z1" или "Z2"). Для алгоритмов шифрования EOFB поле **encryptedSaltingKey** не должно использоваться.

Для ответа сообщением **ACF** конечной точке A в него должны быть включены два маркера ClearTokens, один CT_A для вызывающей конечной точки A и другой CT_B для вызываемой конечной точки B. Поле **ClearToken** CT_A→**tokenOID** должно содержать значение OID "I11".

Привратником G генерируется один Challenge-A и материал ключа шифрования EK_{AG} из общего секрета K_{AG} с помощью процедуры выведения ключа на основе PRF, Challenge-A заменяется на **challenge**, использование процедуры выведения ключа на основе PRF, как описано в пункте 12, где CT_A→**h235Key→secureSharedSecret→keyDerivationOID** должно содержать "AnnexI-HMAC-SHA1-PRF", см. пункт 14, и CT_A→**challenge** должно быть присвоено Challenge-A.

Привратник G, используя алгоритм шифрования, должен зашифровать ключ K_{AB} с помощью EK_{AG}, как $ENC_{EKAG, KSAG, IV}(K_{AB})$, и поместить зашифрованный ключ K_{AB} в CT_A→**h235Key→secureSharedSecret→encryptedSessionKey**.

Должен использоваться расширенный режим шифрования OFB (EOFB) (см. 8.4/H.235.6) с секретным расширенным ключом конечной точки KS_{AG}. Алгоритмы шифрования, которые могут быть применены (см. таблицу 6/H.235.6):

– DES (56 битов) в режиме EOFB, используя OID "Y1": по усмотрению;

– 3DES (168 битов) в режиме внешнего EOFB, используя OID "Z1": по усмотрению;

– AES (128 битов) в режиме EOFB, используя OID "Z2": рекомендуется и является установленным по умолчанию;

– RC2-совместимый (56 битов) в режиме EOFB, используя OID "X1": по усмотрению.

Для режима шифрования EOFB GK G должен сгенерировать случайное начальное значение IV. Для OID "X1", OID "Y1" и OID "Z1" значение IV имеет длину 64 бита и должно быть передано в CT_A→**h235Key→secureSharedSecret→params→iv8**; поскольку значение IV для OID "Z2" имеет длину 128 битов, оно должно быть передано в CT_A→**h235Key→secureSharedSecret→params→iv16**. Алгоритм шифрования должен быть указан в CT_A→**h235Key→secureSharedSecret→algorithmOID** ("X1", "Y1", "Z1" или "Z2").

Идентификатор привратника G должен быть присвоен полю CT_A→**sendersID**, идентификатор конечной точки A должен быть присвоен полю CT_A→**generalID**. Идентификатор конечной точки B должен быть скопирован из CT_B→**generalID** в CT_A→**h235Key**→**secureSharedSecret**→**generalID**.

Если до этого привратником G не было заполнено значение идентификатора конечной точки A в поле endpointIdentifier сообщения **LRQ**, привратник G должен присвоить значение идентификатора конечной точки A полю CT_B→**h235Key**→**secureSharedSecret**→**generalID**.

Для алгоритмов шифрования EOFB поле **encryptedSaltingKey** не должно использоваться.

Как описано в данной Рекомендации, **ClearToken** может использоваться в сочетании с другими профилями защиты, например H.235.1 или H.235.3, в которых также описано развертывание ClearTokens. В таком случае в ClearToken, описанном в данной Рекомендации, должны использоваться также другие поля **ClearToken**. Например, при использовании этой Рекомендации в сочетании с Рек. МСЭ-Т H.235.1 должны быть представлены и использованы поля **timestamp**, **random**, **generalID**, **sendersID** и **dhkey**, как описано в профиле защиты H.235.1.

Идентификатор привратника (GKID) G должен быть помещен в CT_A→**sendersID**, тогда как CT_A→**generalID** должен содержать идентификатор конечной точки A.

Конечной точкой A должен быть распознан маркер CT_A путем проверки поля CT_A→**tokenOID**, которое должно иметь значение "I21". Конечная точка A должна выполнить проверку на давность полученного маркера CT_A с помощью проверки поля **timestamp**. Дальнейшие проверки защиты должны проверять **generalID** и **sendersID** в ClearToken и **generalID** в **secureSharedSecret**. Если полученный маркер CT_A прошел проверку на давность, конечная точка A должна извлечь IV и вычислить EK_{AG} и KS_{AG} для привратника G, как описано выше, используя CT_A→**challenge** вместо Challenge-A, замененное на **challenge** в пункте 12. Чтобы получить $K_{AB,}$ конечной точкой A должно быть расшифровано CT_A→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**.

10.6 Фаза SETUP

Конечной точкой A должен быть распознан маркер CT_A путем проверки поля CT_A→**tokenOID**, которое должно иметь значение "I11". Конечная точка A должна выполнить проверку на давность полученного маркера CT_A с помощью проверки поля **timestamp**. Дальнейшие проверки защиты должны проверять **generalID** и **sendersID** в ClearToken и **generalID** в **secureSharedSecret**. Если полученный маркер CT_A прошел проверку на давность, конечная точка A должна извлечь IV и вычислить EK_{AG} и KS_{AG} для привратника G, как описано выше, используя CT_A→**challenge** вместо Challenge-A. Чтобы получить $K_{AG,}$ конечной точкой A должно быть расшифровано CT_A→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**.

Если полученный маркер CT_A прошел проверку на давность, конечная точка A сможет отправить сообщение SETUP конечной точке B. Данное сообщение SETUP включает маркер CT_B. Сообщение SETUP должно быть защищено (аутентификацией и/или защищенной целостностью) в соответствии с Рек. МСЭ-Т H.235.1 или Рек. МСЭ-Т H.235.3, используя ключ K_{AB} в качестве применяемого общего секрета. Для этого поле **generalID** в хешированном, в соответствии с H.235.1, маркере ClearToken (не CT_B!) не должно быть использованным, за исключением случаев, когда конечная точка A уже имеет значение $EPID_B$ (например, через конфигурацию или сохраненное в памяти с предыдущего соединения). Если конечной точкой A используется значение $EPID_B$ в поле generalID сообщения SETUP, тогда значение sendersID в возвращенном сообщении сигнализации вызова должно быть принято конечной точкой A как истинное значение $EPID_B$.

Конечной точкой B должен быть распознан маркер CT_B путем проверки в ClearToken поля **tokenOID**, которое должно иметь значение "I12".

Конечная точка B должна выполнить проверку на давность полученного маркера CT_B с помощью проверки поля **timestamp**. Дальнейшие проверки защиты должны проверять **sendersID** в ClearToken и **generalID** в **secureSharedSecret**. Если полученный маркер CT_B прошел проверку на давность, конечная точка B должна извлечь IV и вычислить EK_{BH} и KS_{BH} для привратника H, как описано выше, используя CT_B→**challenge** вместо Challenge-B, замененное на **challenge** в пункте 12. Чтобы получить $K_{AB,}$ конечной точкой B должно быть расшифровано CT_B→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**.

В случае если маркер CT_B прошел проверку на давность, конечной точкой B может быть продолжена сигнализация вызова путем отправки команд CALL-PROCEEDING, ALERTING или CONNECT и т. д. В случае если маркер CT_B не прошел проверку на давность или проверка защиты в сообщении

SETUP была не выполнена, конечная точка B должна ответить командой RELEASE-COMPLETE и полю **ReleaseCompleteReason** присвоить значение ошибки защиты, как определено в пункте 11.1/H.235.0.

Если защита среды развернута (см. 6.1/H.235.6), конечные точки A и B должны обменяться половинами ключей Диффи-Хеллмана в соответствии с 8.5/H.235.6 и создать динамический сеансовый ведущий ключ, из которого затем могут быть получены сеансовые ключи среды.

Конечная точка должна включать в сообщения поле **generalID** с присвоенным значением $EPID_A$ и поле **sendersID** с присвоенным значением $EPID_B$ для защиты любых H.225.0 сообщений сигнализации вызова предназначенных для EP A (например, Call Proceeding, Alerting или Connect).

На рисунке 3 показан базовый процесс связи:

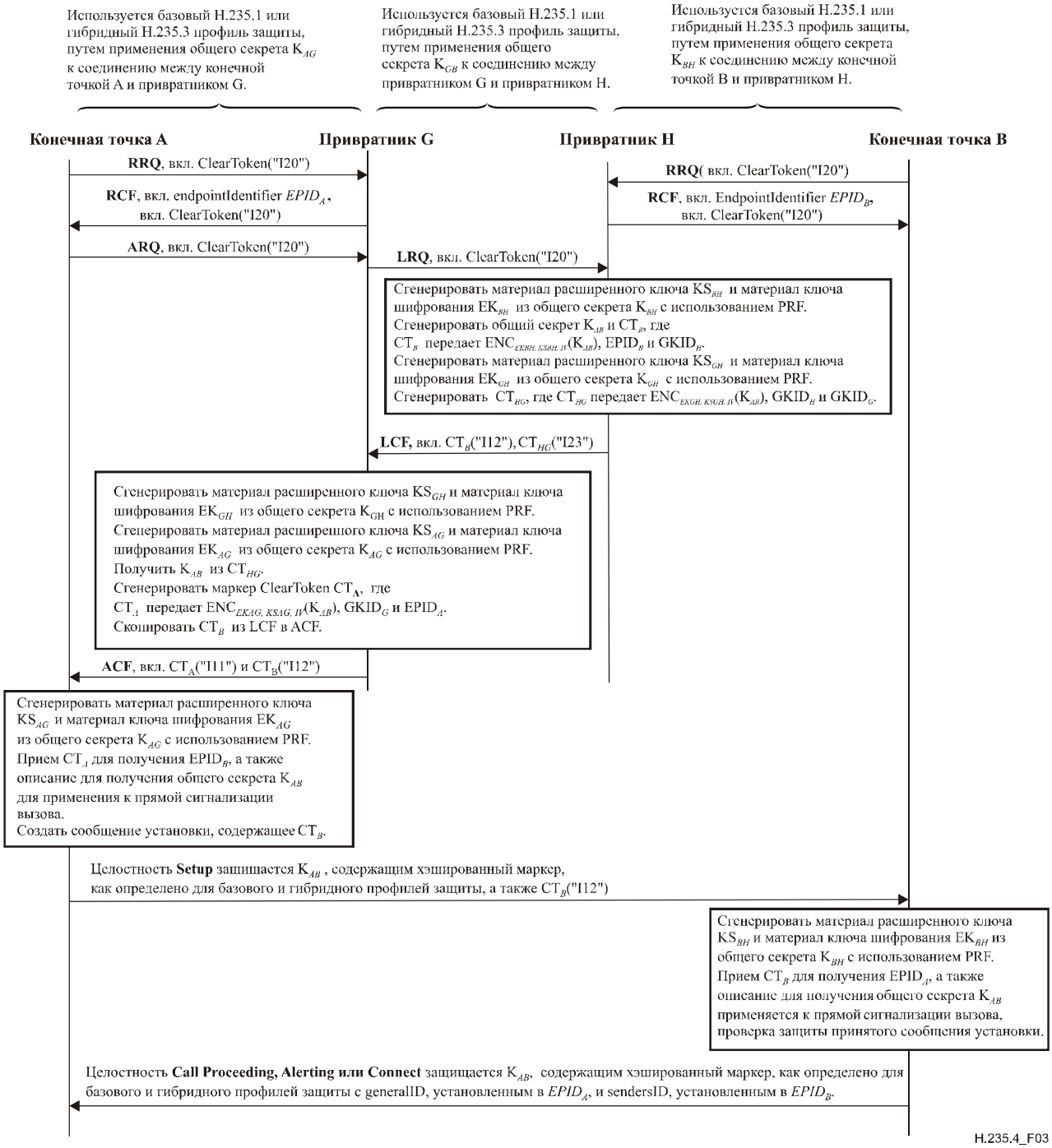

Рисунок 3/H.235.4 – Базовый процесс связи (DRC2)

11 Процедура DRC3 (междоменная среда)

Процедура, описанная в этом пункте, может применяться в междоменных средах, в которых вызывающая конечная точка не может поддерживать алгоритм Диффи-Хеллмана пока оба привратника в вызывающем и вызываемом доменах не смогут выполнить обмен вычисляемыми значениями DH. В такой среде сеансовый ключ вычисляется путем обмена параметрами DH между вызывающим и завершающим привратниками.

11.1 Фаза GRQ/RRQ

В данном сценарии рассмотрены несколько выстроенных в цепочку привратников. Конечными точками, способными поддерживать данный профиль защиты, эта способность должна быть указана во время фазы **GRQ** и/или **RRQ** включением отдельного маркера ClearToken с присвоенным значением "I30" полю **tokenOID**; любые другие поля в данном маркере ClearToken не должны использоваться. Совместимый с H.235.4 привратник, готовый обеспечить необходимые функциональные возможности, должен ответить сообщением **GCF** или **RCF** с отдельным ClearToken, включающим поле **tokenOID** с присвоенным значением "I30", все другие поля в ClearToken не должны использоваться.

11.2 Фаза ARQ

Прежде чем EP A вызовет EP B с помощью процедуры DRC3, EP A отправит сообщение **ARQ** для GK G, сообщение **ARQ** должно содержать отдельный маркер ClearToken с присвоенным значением "I30" полю **tokenOID**, другие поля не должны использоваться.

11.3 Фаза LRQ

На получение сообщения **ARQ** отправленного EP A, GK G отправляет сообщение **LRQ** для GK H, чтобы запросить адрес EP B, так как EP B не принадлежит домену GK G. GK G проверяет маркер ClearToken, перенесенный сообщением **ARQ**, путем поиска значения "I30" в поле **tokenOID**, если GK G поддерживает алгоритм DH, тогда им применяются несколько предварительно настроенных правил, которыми определяется, что должна быть выбрана процедура DRC3.

Затем GK G генерирует сообщение **LRQ** содержащее маркер ClearToken (с CryptoHashedToken) с полем **tokenOID** и присвоенным ему значением "I30", чтобы указать GK H, что необходимо согласование ключа DH. В маркере ClearToken поле **dhkey** заполнено параметрами DH вызывающего устройства (g, p, g^x), которые сгенерированы GK G, другие поля не должны использоваться.

Затем GK G отправляет данное сообщение **LRQ** к GK H. В случае если множество GK, GK G отправляет сообщение **LRQ** к его непосредственно соседнему GK, который в свою очередь пересылает сообщение **LRQ** к своему непосредственно соседнему GK. Процесс пересылки продолжается до тех пор, пока сообщение **LCF** окончательно не достигнет GK H.

При отправке широковещательного сообщения **LRQ** в маркере CryptoToken поле **generalID** не должно использоваться. Если GK G не смог обнаружить конечную точку B, расположенную в удаленном конце сети, GK G должен возвратить сообщение **ARJ** конечной точке A. Связь между двумя привратниками должна быть защищена в соответствии с Рек. МСЭ-Т H.235.1.

Если GK G не поддерживает профиль, GK G имеет свободный выбор – либо перейти к процедуре DRC2, или возвратить сообщение ARJ конечной точке A. Если выбрана процедура DRC2, все последующие фазы, включая фазу **LRQ**, являются такими же, как в DRC2.

11.4 Фаза LCF

После получения сообщения **LRQ** от GK G, если GK H распознал наличие поддержки данной процедуры конечными точками A и B, им должен быть сгенерирован сеансовый ключ K_{AB}, как описано ниже.

Сначала GK H создает случайный Challenge-B, который должен быть присвоен CT_B→**challenge**, CT_B→**h235Key→secureSharedSecret→keyDerivationOID** должно содержать "AnnexI-HMAC-SHA1-PRF", затем используется общий ключ K_{GH} и Challenge-B, чтобы получить материал ключа EK_{GH} и расширенный ключ KS_{GH} с помощью процедуры выведения ключа на основе PRF.

Challenge-B должен быть присвоен полю CT_B→**challenge**, идентификатор привратника GK H должен быть присвоен CT_B→**sendersID**, идентификатор конечной точки EP B должен быть присвоен CT_B→**generalID**. Если в сообщении **LRQ** имеется идентификатор конечной точки EP A в поле

endpointIdentifier, привратником H данный идентификатор должен быть скопирован в CT_B→**h235Key**→**secureSharedSecret**→**generalID**, а также в CT_{HG}→**h235Key**→**secureSharedSecret**→**generalID**.

Привратником GK H создаются два маркера ClearTokens в сообщении **LCF**. Один CT_{HG} с полем **tokenOID**, имеющим присвоенное значение "I33" для GK G, и другой CT_B с полем **tokenOID**, имеющим присвоенное значение "I12" для EP B. GK H генерирует параметры DH вызываемого устройства (g, p, g^y). Вместе с параметрами DH вызываемого устройства полученными из сообщения **LRQ**, GK H должен вычислить сеансовый ключ $K_{AB} = g^{xy} \bmod p$.

В завершении GK H должен зашифровать K_{AB} с помощью EK_{BH} и KS_{BH}, как $ENC_{EKBH, KSBH, IV}(K_{AB})$ и поместить зашифрованный ключ K_{AB} в CT_B→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**, а также поместить параметры DH вызываемого устройства в поле **dhkey** маркера CT_{HG}.

Должен использоваться расширенный режим шифрования OFB (EOFB) (см. 8.4/H.235.6) с секретным расширенным ключом конечной точки KS_{GH}. Алгоритмы шифрования, которые могут быть применены (см. таблицу 6/H.235.6):

– DES (56 битов) в режиме EOFB, используя OID "Y1": по усмотрению;

– 3DES (168 битов) в режиме внешнего EOFB, используя OID "Z1": по усмотрению;

– AES (128 битов) в режиме EOFB, используя OID "Z2": рекомендуется и является установленным по умолчанию;

– RC2-совместимый (56 битов) в режиме EOFB, используя OID "X1": по усмотрению.

Для режима шифрования EOFB привратником H должно быть сгенерировано случайное начальное значение IV. Для OID "X1", OID "Y1" и OID "Z1" значение IV имеет длину 64 бита и должно быть передано в CT_B→**h235Key**→**secureSharedSecret**→ **params**→**iv8**; поскольку значение IV для OID "Z2" имеет длину 128 битов, оно должно быть передано в CT_B→**h235Key**→**secureSharedSecret**→**params**→**iv16**.

Алгоритм шифрования должен быть указан в CT_B→**h235Key**→**secureSharedSecret**→**algorithmOID** ("X1", "Y1", "Z1" или "Z2"). Для алгоритмов шифрования EOFB поле **encryptedSaltingKey** не должно использоваться.

GK H отправляет сообщение **LCF** для GK G. Если представлено множество GK, сообщение **LCF** будет передано способом пересылки. Во время прохождения этого пути каждый GK получает сообщение **LCF** от вышестоящего непосредственного соседа, проверяет сообщение **LCF** содержащее CT_{HG} и пересылает его к своему нижестоящему непосредственному соседу.

Если GK H не поддерживает алгоритм DH или политика защиты не разрешена для процедуры DRC3, произойдет откат к процедуре DRC2. Поэтому фаза **LCF** и все последующие фазы такие же, как в процедуре DRC2.

11.5 Фаза ACF

После получения сообщения **LCF** GK G распознает поле **tokenOID** в отдельном маркере ClearToken по присвоенному значению "I33", получает DH вызываемого устройства и создает маркер ClearToken, обозначающий CT_A с присвоенным значением полю **tokenOID** "I11" способом, указанным ниже.

Сначала GK H создает случайный Challenge-A, который должен быть присвоен CT_A→**challenge**, CT_A→**h235Key**→**secureSharedSecret**→**keyDerivationOID** должно содержать "AnnexI-HMAC-SHA1-PRF", затем используется общий ключ K_{AG} и Challenge-A, чтобы получить материал ключа EK_{AG} и расширенный ключ KS_{AG} с помощью процедуры выведения ключа на основе PRF.

Затем GK G использует параметры DH вызываемого устройства, которые сохранены во время фазы **LRQ**, и в сочетании с параметрами DH вызываемого устройства вычисляется сеансовый ключ $K_{AG} = g^{xy} \bmod p$.

GK G копирует маркер ClearToken CT_B из сообщения **LCF** в сообщение **ACF**, полю **tokenOID** которого должно быть присвоено "I12".

В завершении GK G шифрует ключ K_{AB} с помощью ключа EK_{AG} и KS_{AG}, как $ENC_{EKAG, KSAG, IV}(K_{AB})$, затем помещает зашифрованный K_{AB} в CT_A→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**, и копирует CT_B из сообщения **LCF** в сообщение **ACF**.

Должен использоваться расширенный режим шифрования OFB (EOFB) (см. 8.4/H.235.6) с секретным расширенным ключом конечной точки KS_{AG}.

Алгоритмы шифрования, которые могут быть применены (Таблица 6/H.235.6):

– DES (56 битов) в режиме EOFB, используя OID "Y1": по усмотрению;

– 3DES (168 битов) в режиме внешнего EOFB, используя OID "Z1": по усмотрению;

– AES (128 битов) в режиме EOFB, используя OID "Z2": рекомендуется и является установленным по умолчанию;

– RC2-совместимый (56 битов) в режиме EOFB, используя OID "X1": по усмотрению.

Для режима шифрования EOFB GK G должен сгенерировать случайное начальное значение IV. Для OID "X1", OID "Y1" и OID "Z1" значение IV имеет длину 64 бита и должно быть передано в CT_A→**h235Key**→**secureSharedSecret**→**params**→**iv8**; поскольку значение IV для OID "Z2" имеет длину 128 битов, оно должно быть передано в CT_A→**h235Key**→**secureSharedSecret**→**params**→**iv16**. Алгоритм шифрования должен быть указан в CT_A→**h235Key**→**secureSharedSecret**→**algorithmOID** ("X1", "Y1", "Z1" или "Z2").

Если обнаружено, что поле **tokenOID** маркера ClearToken (в сообщении **LCF**) имеет значение "I23", может полагаться, что произошел откат к процедуре DRC2 и GK G будет иметь возможность свободного выбора принимать или нет политику защиты GK H. Если политика принята, фаза **ACF** и последующая фаза Setup будут такими же, как в процедуре DRC2. Иначе последует ответ с соответствующим отклоняющим сообщением, указывающим ошибку защиты, с присвоенной причиной отклонения в поле securityDenial.

GK G отправит сообщение **ACF** для EP A.

11.6 Фаза SETUP

Конечной точкой A должен быть распознан маркер CT_A путем проверки поля CT_A→**tokenOID**, которое должно иметь значение "I11". Конечная точка A должна выполнить проверку на давность полученного маркера CT_A с помощью проверки поля **timestamp**. Дальнейшие проверки защиты должны проверять **generalID** и **sendersID** в ClearToken и **generalID** в **secureSharedSecret**. Если полученный маркер CT_A прошел проверку на давность, конечная точка A должна извлечь IV и вычислить EK_{AG} и KS_{AG} для привратника G, как описано выше, используя CT_A→**challenge** вместо Challenge-A. Чтобы получить $K_{AG,}$ конечной точкой A должно быть расшифровано CT_A→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**.

Если полученный маркер CT_A прошел проверку на давность, конечная точка A сможет отправить сообщение SETUP конечной точке B. Данное сообщение SETUP включает маркер CT_B. Сообщение SETUP должно быть защищено (аутентификацией и/или защищенной целостностью) в соответствии с Рек. МСЭ-Т H.235.1 или Рек. МСЭ-Т H.235.3, используя ключ K_{AB} в качестве применяемого общего секрета. Для этого поле **generalID** в хешированном, в соответствии с H.235.1, маркере ClearToken (не CT_B!) не должно быть использованным, за исключением случаев, когда конечная точка A уже имеет значение $EPID_B$ (например, через конфигурацию или сохраненное в памяти с предыдущего соединения). Если конечной точкой A используется значение $EPID_B$ в поле **generalID** сообщения SETUP, тогда значение **sendersID** в возвращенном сообщении сигнализации вызова должно быть принято конечной точкой A как истинное значение $EPID_B$.

Конечной точкой B должен быть распознан маркер CT_B путем проверки в ClearToken поля **tokenOID**, которое должно иметь значение "I12".

Конечная точка B должна выполнить проверку на давность полученного маркера CT_B с помощью проверки поля **timestamp**. Дальнейшие проверки защиты должны проверять **sendersID** в ClearToken и **generalID** в **secureSharedSecret**. Если полученный маркер CT_B прошел проверку на давность, конечная точка B должна извлечь IV и вычислить EK_{BH} и $KS_{BH,}$ используя CT_B→**challenge** вместо Challenge-B. Чтобы получить $K_{AB,}$ конечной точкой B должно быть расшифровано CT_B→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**.

В случае если маркер CT_B прошел проверку на давность, конечной точкой B может быть продолжена сигнализация вызова путем отправки команд CALL-PROCEEDING, ALERTING или CONNECT и т. д. В случае если маркер CT_B не прошел проверку на давность или проверка защиты в сообщении SETUP была не выполнена, конечная точка B должна ответить командой RELEASE-COMPLETE и полю **ReleaseCompleteReason** присвоить значение ошибки защиты, как определено в пункте 11.1/H.235.0.

Если защита среды развернута (см. 6.1/H.235.6), конечные точки A и B должны обменяться половинами ключей Диффи-Хеллмана в соответствии с 8.5/H.235.6 и создать динамический сеансовый ведущий ключ, из которого затем могут быть получены сеансовые ключи среды.

Конечная точка должна включать в сообщения поле **generalID** с присвоенным значением $EPID_A$ и поле **sendersID** с присвоенным значением $EPID_B$ для защиты любых H.225.0 сообщений сигнализации вызова, предназначенных для EP A (например, Call Proceeding, Alerting или Connect).

На рисунке 4 показан базовый процесс связи:

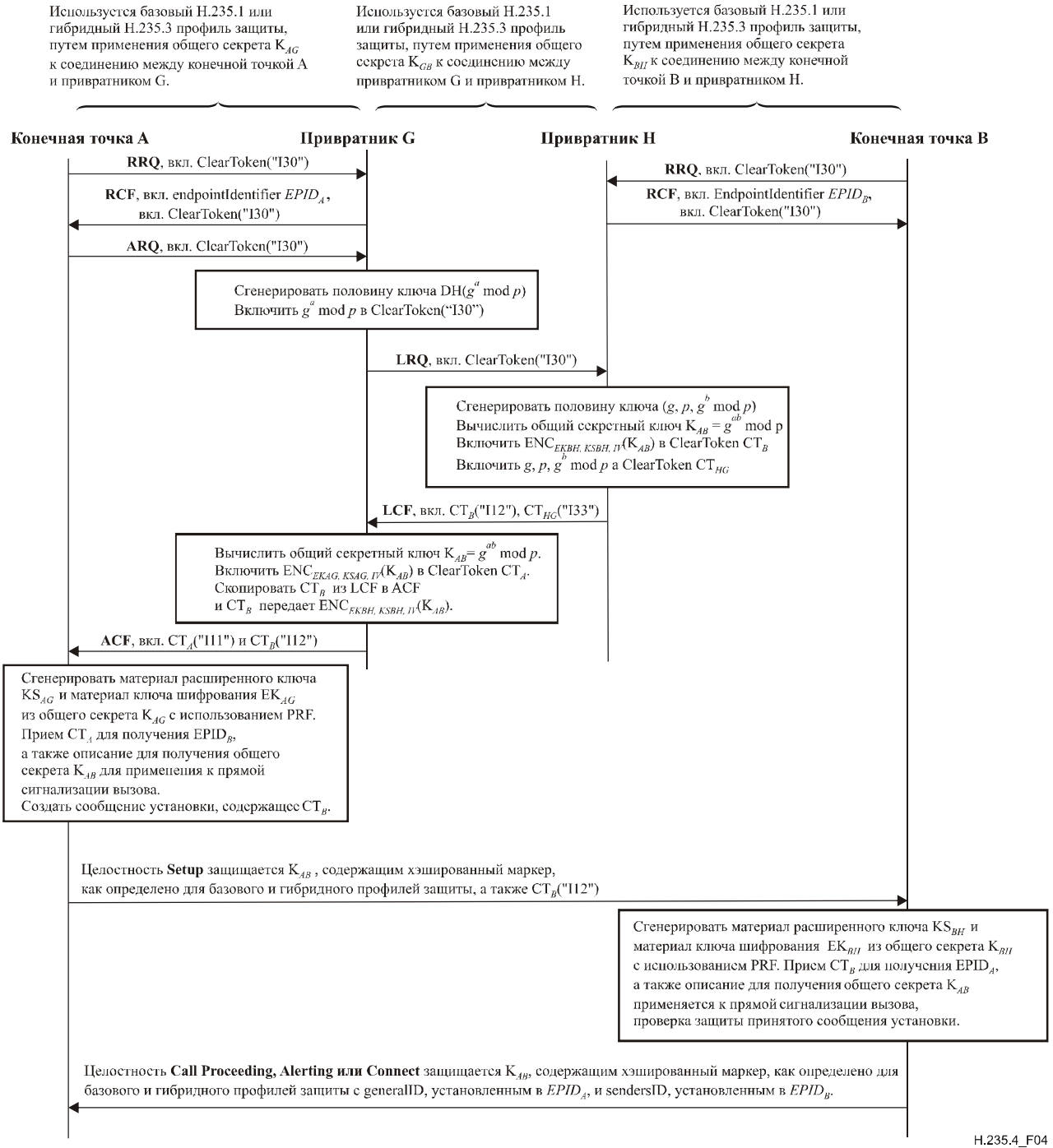

Рисунок 4/H.235.4 – Процесс связи в процедуре DRC3

12 Процедура выведения ключа на основе PRF

В этом пункте описывается процедура, которая определяет, как получить материал ключа из общего секрета и другие параметры.

Процедура, описанная в данном пункте, позволяет вычислять ключ шифрования и расширенный ключ из общего ключа. Процедура является унифицированной и независимой от общего секрета (K_{AG}, K_{BH} или K_{GH}).

Чтобы получить целевой ключевой материал (например, EK_{AG}), процедура PRF (см. пункт 10/H.235.0) должна использоваться с параметрами, полученными из таблицы 1, где параметру *inkey* присвоен соответствующий общий ключ (например, K_{AG}), и параметру *label* должна быть присвоена соответствующая константа (например, 0x2AD01C64 || **challenge-A)**, где символ **||** обозначает связь. Параметру *outkey_len* должно быть присвоено значение необходимой длины целевых данных ключа, которая зависит от выбранного алгоритма шифрования.

ПРИМЕЧАНИЕ. – Для EK_{AG}, KS_{AG}, EK_{BH} и KS_{BH} 32-битные постоянные целочисленные числа (т. е. 0x2AD01C64) берутся из десятичных цифр числа *e* (т. е. 2,71828...), а для EK_{GH} и KS_{GH}, 32-битные постоянные целочисленные числа берутся из десятичных цифр числа π (т. е. 3,14159...). Для EK_{AG}, EK_{BH}, KS_{AG}, и KS_{BH}, 32-битные целые числа берутся из блоков 9 десятичных цифр, соответственно первый, второй, четвертый и седьмой блоки. Значение для EK_{GH} берется из первых 10 десятичных цифр числа π, тогда как для KS_{GH} берется из 8 последовательных десятичных цифр π.

Таблица 1/H.235.4 – Вычисление ключей шифрования и расширенных ключей из общего секрета

Целевой Ключ	PRF inkey	Константа || вызов
EK_{AG}	K_{AG}	0x2AD01C64 || **Challenge-A**
KS_{AG}	K_{AG}	0x150533E1 || **Challenge-A**
EK_{BH}	K_{BH}	0x1B5C7973 || **Challenge-B**
KS_{BH}	K_{BH}	0x39A2C14B || **Challenge-B**
EK_{GH}	K_{GH}	0x54655307 || **Challenge-G**
KS_{GH}	K_{GH}	0x35855C60 || **Challenge-G**

13 Процедура выведения ключа на основе FIPS-140

Возможно, в данном пункте будет описана процедура, которая определяет, как получить материал ключа из общего секрета и другие параметры с помощью совместимого с FIPS-140 модуля шифрования. Эта тема остается предметом дальнейших исследований.

14 Список идентификаторов объектов

Таблица 2/H.235.4 – Идентификаторы объектов используемые в H.235.4

Ссылка на идентификатор объекта	Значение идентификатора объекта	Описание
"I10"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 48}	Используется в процедуре DRC1 в течение фаз GRQ/RRQ, GCF/RCF и ARQ, чтобы EP/GK могли указать возможность поддержки DRC1.
"I11"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 49}	Используется в процедурах DRC1, DRC2 и DRC3 для поля tokenOID маркера ClearToken, указывающий, что ClearToken CT_A содержит сквозной ключ для вызывающего.
"I12"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 50}	Используется в процедурах DRC1, DRC2 и DRC3 для поля tokenOID маркера ClearToken, указывающий, что ClearToken CT_B содержит сквозной ключ для вызываемого.
"I13"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 52}	Используется в процедуре DRC1 для поля tokenOID маркера ClearToken, передаваемого между привратниками, указывающий, что ClearToken CT_{HG} содержит ключ шифрования для вызывающего привратника.
"I20"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 53}	Используется в процедуре DRC2 в течение фаз GRQ/RRQ, GCF/RCF и ARQ, чтобы EP/GK могли указать возможность поддержки DRC2.
"I23"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 56}	Используется в процедуре DRC2 для поля tokenOID маркера ClearToken CT_{HG}, передаваемого между привратниками, указывающий, что ClearToken содержит ключ шифрования для вызывающего привратника.
"I30"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 34}	Для использования в отдельном ClearToken в фазах GRQ/RRQ, GCF/RCF, ARQ, чтобы указать поддержку процедуры DRC3. Для использования в отдельном ClearToken в LRQ, чтобы указать перенесенные параметры DH вызывающего.
"I33"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 37}	Для использования в отдельном ClearToken в LCF, чтобы указать перенесенные параметры DH вызываемого.
"Annex I -HMAC-SHA1-PRF"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 51}	Используется в процедурах DRC1, DRC2 и DRC3 для поля keyDerivationOID в V3KeySyncMaterial, чтобы указать применяемый метод извлечения ключа в пункте 12, используя псевдослучайную функцию HMAC-SHA1.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

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

Отпечатано в Швейцарии
Женева, 2007 г.