МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

H.235.7

(09/2005)

СЕРИЯ H: АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

Инфраструктура аудиовизуальных услуг – Системные аспекты

Безопасность H.323: Использование протокола управления ключами MIKEY для протокола защиты транспорта в режиме реального времени (SRTP) в H.235

Рекомендация МСЭ-Т H.235.7

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 справочников 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.235.7

Безопасность H.323: Использование протокола управления ключами MIKEY для протокола защиты транспорта в режиме реального времени (SRTP) в H.235

Резюме

Целью данной Рекомендации является описание процедур защиты для систем на основе H.323/H.235 при использовании протокола управления ключами MIKEY совместно с протоколом защиты транспорта в режиме реального времени (SRTP).

В предыдущих версиях Рекомендаций подсерии H.235 данный профиль содержался в Приложении G/H.235. В Дополнениях IV, V, VI к Рекомендации H.235.0 приводятся таблицы соответствий между пунктами, рисунками и таблицами версий 3 и 4 Рекомендаций H.235.

Источник

Рекомендация МСЭ-Т H.235.7 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

Шифрование медиа, управление ключами MIKEY, защита мультимедиа, протокол защиты транспорта в режиме реального времени, профиль защиты, SRTP.

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
2		Справочные документы	1
	2.1	Нормативные справочные документы	1
	2.2	Информативные справочные документы и библиография	2
3		Определения	2
4		Символы и сокращения	2
5		Соглашения о терминах	4
6		Введение	4
7		Обзор и сценарии	5
	7.1	Функционирование протокола MIKEY на "уровне сессии"	6
	7.2	Функционирование протокола MIKEY на "уровне медиа"	7
	7.3	Согласование возможностей MIKEY	8
8		Профиль защиты, использующий схему симметричного шифрования	9
	8.1	Завершение вызова H.323	14
	8.2	Смена ключей шифрования TGK и обновление CSB	15
	8.3	Поддержка туннелирования H.245	16
	8.4	Алгоритмы SRTP	16
	8.5	Список идентификаторов объекта	17
9		Профиль защиты, использующий схему ассиметричного шифрования	17
	9.1	Завершение вызова H.323	21
	9.2	Смена ключа шифрования TGK и обновление CSB	21
	9.3	Поддержка туннелирования H.245	23
	9.4	Алгоритмы SRTP	23
	9.5	Список идентификаторов объекта	23
Дополнение I – Опция MIKEY-DHHMAC			23
	I.1	Завершение вызова H.323	27
	I.2	Смена ключа шифрования TGK и обновление CSB	28
Дополнение II – Использование H.235.4 для создания предварительного общего секрета			30
	II.1	Завершение вызова H.323	32
	II.2	Смена ключей шифрования TGK и обновление CSB	32

Введение

Целью данной Рекомендации является описание процедур защиты для систем на основе H.323/H.235 при использовании протокола управления ключами MIKEY комитета IETF совместно с протоколом защиты SRTP IETF.

Данная Рекомендация была создана как профиль защиты Рек. МСЭ-Т H.235, т. е. она предлагается в качестве опции и может дополнять другие возможности защиты мультимедиа Рекомендации МСЭ-Т H.235.6.

В данной Рекомендации допускается возможность использования протокола защиты медиа SRTP, в котором протокол управления ключами MIKEY передает необходимые ключи и параметры защиты между конечными точками – участниками на сквозной основе. Данная Рекомендация может быть использована в рамках домена H.323 между системами H.323, поддерживающими H.235.7. В данной Рекомендации определяются расширения протокола защиты на RAS и сигнализации вызова H.225.0, а также H.245, вместе с соответствующими процедурами. Более того, в данной Рекомендации обеспечиваются возможности для поддержки межсетевого взаимодействия с объектами SIP IETF, применяющими протокол управления ключами MIKEY и протокол SRTP.

Рекомендация МСЭ-Т H.235.7

Безопасность H.323: Использование протокола управления ключами MIKEY для протокола защиты транспорта в режиме реального времени (SRTP) в H.235

1 Сфера применения

Целью данной Рекомендации является описание процедур защиты для систем на основе H.323/H.235 при использовании протокола управления ключами MIKEY совместно с протоколом защиты SRTP.

Данный профиль защиты предлагается в качестве опции и может дополнять другие возможности защиты медиа Рекомендации H.235.6.

2 Справочные документы

2.1 Нормативные справочные документы

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

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

– ITU-T Recommendation H.235.0 (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*.

– Рекомендация МСЭ-Т H.235.4 (2005 г.), *Защита H.323: Защита вызовов с прямой и избирательной маршрутизацией*.

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

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

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

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

– IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

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

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

2.2 Информативные справочные документы и библиография

– IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

– IETF RFC 2327 (1999), *SDP: Session description protocol*.

– IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method*.

– IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

– IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP)*.

– IETF RFC 4566 (2006), M. Handley, Van Jacobson, C. Perkins: *SDP: Session Description Protocol*, draft-ietf-mmusic-sdp-new-24.txt.

– IETF RFC 4567 (2006), J. Arkko, E. Carrara et al: *Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)*, Internet Draft draft-ietf-mmusic-kmgmt-ext-14.txt, Work in Progress.

– IETF RFC 4650 (2006), M. Euchner: *HMAC-authenticated Diffie-Hellman for MIKEY*, Internet Draft draft-ietf-msec-MIKEY-DHHMAC-11.txt, Work in Progress.

3 Определения

Отсутствуют.

4 Символы и сокращения

В данной Рекомендации используются следующие сокращения:

a, b, e, d	private DH key of EP A, EP B, GK E, GK D	Частный ключ DH (Диффи-Хеллмана) конечной точки A, конечной точки B, привратника E, привратника D (EP A, EP B, GK E, GK D)
Cert	digital certificate (see RFC 3830)	Цифровой сертификат (см. RFC 3830)
CP/C	CallProceeding-to-Connect	Сообщение CallProceeding-to-Connect системной процедуры начала установления связи
CSB	Crypto Session Bundle (see RFC 3830)	Несколько криптографических сессий (в которых используются общие параметры защиты) (см. RFC 3830)
CT_B, CT_A	ClearToken for endpoint B, ClearToken for endpoint A (see H.235.4)	Маркер ClearToken для конечной точки B, маркер ClearToken для конечной точки A (см. H.235.4)
DRC1	Direct-routed Call (see H.235.4)	Прямой вызов (см. H.235.4)
$ENC_k(x)$	Encryption of *X* using key *k*	Шифрование *X* с использованием ключа *k*
env_key	Envelope key (RFC 3830) between endpoint B and endpoint A	Ключ огибающей (RFC 3830) между конечными точками B и A
EP	Endpoint	Конечная точка
ESC	H.245 EndSessionCommand	Команда H.245 EndSessionCommand
DH	Diffie-Hellman	Алгоритм шифрования Диффи-Хеллмана
DH_A	DH half-key of endpoint A	Половина ключа DH конечной точки A
DH_B	DH half-key of endpoint B	Половина ключа DH конечной точки B
g^a, g^b	Diffie-Hellman half-key of EP A, EP B	Половина ключа Диффи-Хеллмана EP A, EP B
g^e, g^d	Diffie-Hellman half-key of GK E, GK D	Половина ключа Диффи-Хеллмана GK E, GK D
GK	Gatekeeper	Привратник
HDR	MIKEY header payload (see RFC 3830)	Полезная нагрузка заголовка MIKEY (см. RFC 3830)

ID_A, ID_B	Identity (i.e., endpoint ID) of endpoint A, Identity of endpoint B	Особенность (т. е. идентификатор (ID) конечной точки) конечной точки A, особенность конечной точки B
IETF	Internet Engineering Task Force	Комитет по инженерным вопросам Internet, комитет IETF
Imsg	MIKEY message of the initiator (see RFC 3830)	Сообщение MIKEY инициатора (см. RFC 3830)
KEMAC	MIKEY KEMAC payload message (see RFC 3830)	Сообщение полезной нагрузки KEMAC MIKEY (см. RFC 3830)
MAC(*k*, *x*)	Keyed MAC on *x* using key *k*	Закодированный MAC (код аутентификации сообщения) по *x* с использованием ключа *k*
Ma	MIKEY authentication key (see RFC 3830)	Ключ аутентификации MIKEY (см. RFC 3830)
Me	MIKEY encryption key (see RFC 3830)	Ключ шифрования MIKEY (см. RFC 3830)
MIKEY	Multimedia Internet Keying	Использование ключей для мультимедийного интернета
NTP	Network Time Protocol	Протокол сетевого времени, протокол NTP
PKE	MIKEY PKE payload message (see RFC 3830)	Сообщение полезной нагрузки MIKEY PKE (см. RFC 3830)
PKI	Public-Key Infrastructure	Инфраструктура открытых ключей
PRF	Pseudo-Random Function (MIKEY-PRF, see RFC 3830 sections 4.1.2-4.1.4)	Псевдослучайная функция (MIKEY-PRF, см. разделы 4.1.2–4.1.4 RFC 3830)
Rand	random nonce (see RFC 3830)	Случайное значение, используемое только однажды (см. RFC 3830)
Rmsg	MIKEY message of the responder (see RFC 3830)	Сообщение MIKEY ответчика (см. RFC 3830)
rand()	random value	Случайное значение
RSA	Rivest, Shamir and Adleman (public key algorithm)	Алгоритм шифрования открытым ключом (Райвеста, Шамира и Адлемана)
sa, *sb*	shared secret among endpoint A and GK, shared secret among endpoint B and GK	Общий секрет у конечной точки A и GK, общий секрет у конечной точки B и GK
sl	shared secret among gatekeepers	Общий секрет у привратников
SDP	Session Description Protocol	Протокол описания сессии
SHA1	Secure Hash Algorithm 1 (ISO/IEC 10118-3)	Алгоритм аутентификации и проверки целостности информации (ИСО/МЭК 10118-3)
SIP	Session Initiation Protocol	Протокол инициации сессии, протокол SIP
SP	Security Policy (see RFC 3830)	Политика защиты (см. RFC 3830)
SRTCP	Secure Real-time Transport Control Protocol	Протокол контроля защиты транспорта в режиме реального времени, протокол SRTCP
SRTP	Secure Real-time Transport Protocol (see RFC 3711)	Протокол защиты транспорта в режиме реального времени, протокол SRTP (см. RFC 3711)
SSRC	Synchronization source (RTP)	Источник синхронизации (RTP)
T	Timestamp (see RFC 3830)	Отметка времени (см. RFC 3830)
TGK	Traffic Generating Key (see RFC 3830) between endpoint A and endpoint B	Ключ, генерирующий трафик (см. RFC 3830) между конечной точкой A и конечной точкой B
V	Verification message field (see RFC 3830)	Верификационное поле сообщения (см. RFC 3830)
ZZ_{AB}	dynamic shared H.323 secret ZZ_{AB}	Динамический общий секрет ZZ_{AB} H.323
{}	Zero, one or more occurrences	Ноль, один или более случаев
[]	Optional element	Дополнительный элемент

5 Соглашения о терминах

В тексте данной Рекомендации ссылки на идентификаторы объекта даются в символическом виде (например, "G1"), действительные числовые значения идентификаторов объекта приводятся в пп. 8.5 и 9.5, более подробную информацию см. в пункте 5/H.235.0.

В таблице 1 описаны пять протоколов управления ключами MIKEY, ссылки на которые встречаются в тексте данной Рекомендации:

Таблица 1/H.235.7 – Протоколы управления ключами MIKEY

Протокол MIKEY	Описание	Значение OID	Идентификатор параметра	Применение
MIKEY	Любой протокол MIKEY	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 76}	76	Обязателен для применения
MIKEY-PS	Протокол распределения симметричных ключей с использованием предварительных общих симметричных ключей и HMAC, (см. RFC 3830).	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 72}	72	Обязателен для применения
MIKEY-DHHMAC	Протокол согласования ключей Диффи-Хеллмана с использованием предварительных общих симметричных ключей и HMAC; (см. RFC 4650).	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 73}	73	Дополнительный
MIKEY-PK-SIGN	Протокол распределения открытого ключа (на основе RSA) с использованием цифровых подписей; (см. RFC 3830).	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 74}	74	Обязателен для применения
MIKEY-DH-SIGN	Протокол согласования ключей Диффи-Хеллмана с использованием цифровой подписи; (см. RFC 3830).	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 75}	75	Дополнительный

MIKEY (сравните 1-й ряд таблицы 1) относится ко всей группе протоколов MIKEY в общем, без указания на какой-либо определенный вариант протокола управления ключами MIKEY как, например, MIKEY-PS, MIKEY-DHHMAC, MIKEY-PK-SIGN или MIKEY-DH-SIGN. Указанная реализация протокола MIKEY должна выполнять обработку сообщений MIKEY таких, как общая полезная нагрузка заголовка MIKEY (RFC 3830, пункт 6.1), но не обязательно требует применения определенного протокола управления ключами или применения определенной полезной нагрузки информации MIKEY. В тех случаях, когда конечной точке H.323 не известно, какой вариант протокола MIKEY используется в действительности, необходимо использовать соответствующий идентификатор объекта (OID) и идентификатор параметра. Во всех других случаях рекомендуется использовать специальный идентификатор объекта (OID) и идентификатор параметра действующего протокола управления ключами MIKEY.

6 Введение

Представляет интерес использование функций защиты "Протокола защиты в режиме реального времени" SRTP IETF из Рек. МСЭ-Т H.235. Наряду с тем, что в предыдущих версиях Рекомендации H.235 уже представлены различные функции защиты, такие, как шифрование голоса с использованием блочных шифров и ограниченная аутентификация RTP (опция анти-спам), есть серьезные основания для использования SRTP:

– использование поточного шифра для улучшения показателей работы, надежности и защиты;

– взаимодействовать с другими оконечными устройствами SRTP такими, как оконечные устройства медиа на основе SIP.

ПРИМЕЧАНИЕ. – В данной Рекомендации не рассматриваются процедуры для межсетевого взаимодействия с SIP в области защиты (RFC 3261); это является предметом дальнейшего изучения.

– обеспечивать более высокий уровень защиты для защиты RTCP;

– достигать лучших показателей целостности, охватывающей весь пакет RTP/RTCP;

– использовать современный алгоритм шифрования AES;

– использовать ключи шифрования/аутентификации сессии, полученные из псевдослучайной функции на обоих концах.

Более того, существует необходимость в обеспечении управления ключами на основе RSA в дополнение к схемам согласования ключей Диффи-Хеллмана, предоставляемых H.235. Также представляются полезными методы управления ключами, основанные не на PKI, в случаях, когда инфраструктуры открытого ключа не подходят. Также интерес представляет аспект законного прослушивания в контексте управлении ключами.

Комитет IETF также попытался определить схему управления ключами MIKEY (RFC 3830), способную поддерживать режим реального времени. Эта общая схема управления ключами хорошо работает вместе с протоколом SRTP и способна генерировать главные ключи (TGK), а также ключи трафика сессии на сквозной основе или, возможно, на основе решений конец-середина/переход-переход (end-to-middle/hop-by-hop). MIKEY является оптимизированным протоколом управления ключами, реализация которого ограничивается двумя сообщениями, что делает его идеальным для быстрого установления соединения в H.323.

В данной Рекомендации рассматриваются процедуры защиты для использования протоколов управления ключами MIKEY в H.323/H.235 для обеспечения защиты медиа SRTP. Следует заметить, что, возможно, существуют другие альтернативные способы поддержки протокола SRTP в H.323/H.235, однако такие меры не являются предметом данной Рекомендации и являются предметом дальнейшего изучения.

Концепция использования протоколов управления ключами MIKEY аналогична подходу, описанному в RFC 4567, где протокол SIP (RFC 3261) передает протокол MIKEY внутри протокола SDP (RFC 2327, RFC 4566 и RFC 3264).

В данной Рекомендации описываются два профиля защиты с процедурами защиты для двух различных инфраструктур защиты:

– инфраструктура защиты на основе симметричных ключей, поддерживающая многочисленные привратники (см. пункт 8); и

– инфраструктура защиты на основе асимметричных ключей (PKI), поддерживающая многочисленные привратники (см. пункт 9).

7 Обзор и сценарии

На рисунке 1 представлен общий сценарий, который исследуется в данной Рекомендации. Частью данного сценария являются, по крайней мере, две отдельные конечные точки A и B H.323. Эти конечные точки могут представлять собой оконечные устройства H.323 или медийные шлюзы H.323, последние обладают потенциальной возможностью взаимодействовать с другими сетями с коммутацией пакетов или без нее. Кроме того, предполагается, что частью сетевого окружения является, по крайней мере, один привратник. В случае если привратник только один, предполагается, что конечные точки H.323 находятся только внутри зоны данного единственного привратника. В случае если привратников несколько и они составляют цепочку, конечные точки H.323 могут быть размещены в зонах разных привратников. Более того, предполагается, что конечные точки H.323 взаимодействуют напрямую на сквозной основе, используя протокол медиа RTP.

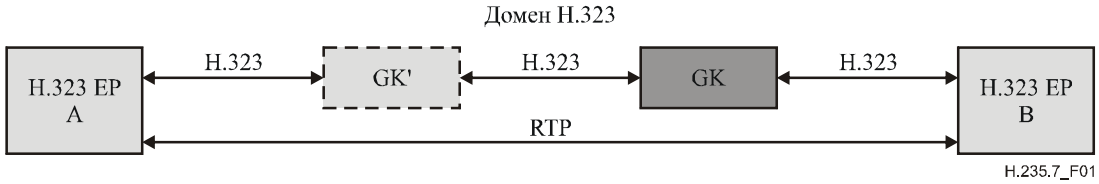

Рисунок 1/H.235.7 – Сценарий

На рисунке 2 представлен общий сценарий защиты с отображением применения протоколов управления ключами MIKEY и протокола защиты медиа SRTP. Протоколы управления ключами MIKEY проходят между конечными точками H.323 A и B; протоколы управления ключами MIKEY инкапсулируются в контейнеры внутри квитирования сигнализации H.245 (Terminal Capability Set, Request Mode, Open Logical Channel handshakes и MiscellaneousCommand) и остаются прозрачными для всех промежуточных привратников.

Следует заметить, что, в действительности, конечная точка H.323 может быть шлюзом. Например, такой шлюз может обеспечивать функцию межсетевого обмена для слаженной работы с системами на основе SIP. В этом случае шлюз не обязательно завершает выполнение MIKEY, но может передавать MIKEY далее и расширять MIKEY для верного сквозного управления ключами между участвующими в процессе мультимедийными оконечными устройствами, таким образом поддерживая сквозную безопасность медиа с SRTP. Данный подход мог бы поддерживать межсетевое взаимодействие в области защиты между системами на основе H.323/H.235 и SIP. Подробное описание функциональных возможностей межсетевого взаимодействия или технические характеристики таких шлюзов не являются предметом данной Рекомендации и являются объектом дальнейшего изучения.

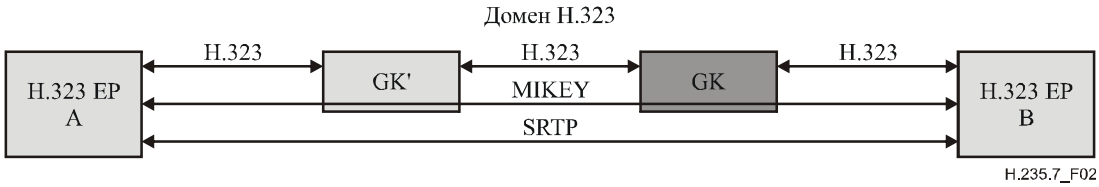

Рисунок 2/H.235.7 – Сценарий защиты с MIKEY и SRTP

Реализация всех протоколов управления ключами, описанных в данной Рекомендации, проходит в два этапа:

– Этап 1 проходит во время фазы RAS H.225.0 и сигнализации вызова. Для протоколов MIKEY для симметричного ключа (MIKEY-PS или MIKEY-DHHMAC) на этой стадии происходит создание сквозного общего секрета ZZ_{AB} между конечными точками A и B, который используется как предварительный общий секрет для MIKEY. Для протоколов MIKEY для асимметричных ключей (MIKEY-PK-SIGN и MIKEY-DH-SIGN) на данном этапе происходит создание динамических общих секретов между конечной точкой и следующим переходом (обычно служебным привратником); динамический общий секрет не относится к протоколу MIKEY, но служит для обеспечения защиты сигнализация вызова H.225.0 между конечной точкой и следующим переходом.

– Этап 2 проходит во время фазы сигнализация вызова H.225.0/H.245. На данном этапе происходит согласование и передача протокола MIKEY (MIKEY-PS, MIKEY-DHHMAC, MIKEY-PK-SIGN или MIKEY-DH-SIGN) между конечными точками A и B, и создается MIKEY TGK. Во время этапа 2 конечные точки MIKEY могут также реализовывать смену шифровальных ключей MIKEY и протокол обновления ключей для обновления TGK. Далее во время этапа 2 может происходить завершение соединения и сброс материала ключей (TGK).

7.1 Функционирование протокола MIKEY на "уровне сессии"

Протоколы управления ключами MIKEY могут функционировать на "уровне сессии", т. е. TGK MIKEY применяется более чем к одному потоку медиа. Рекомендуется запускать MIKEY на уровне сессии во время квитирования **TerminalCapability**.

TerminalCapabilitySet должно использовать **h235SecurityCapability**, где **genericH235SecurityCapability** используется внутри **encryptionAuthenticationAndIntegrity** следующим образом:

– **capabilityIdentifier** должно содержать в **standard** один из идентификаторов объекта MIKEY;

– **maxbitRate** и **collapsing** не используются;

– при использовании протокола MIKEY на "уровне сессии" для всех логических каналов в **nonCollapsing** должны быть выставлены следующие значения **GenericParameters**:

  • **parameterIdentifier**: в **standard,** для обозначения протокола MIKEY на "уровне сессии" используется значение 0.

  • **parameterValue** с сообщением MIKEY (I или R) в двоичном коде внутри **octetString**.

  • **supersedes** не заполняется/не используется.

– **nonCollapsingRaw** не используется;

– **transport** (не используется или используется с заданными по умолчанию транспортными параметрами).

OpenLogicalChannel и **OpenLogicalChannelAck** не должны использовать **encryptionSync** для реализации протокола MIKEY на "уровне сессии". **RequestMode** также не должно использовать **genericModeParameters ModeElement** для протокола MIKEY, когда он реализуется на "уровне сессии".

MiscellaneousCommand должно использовать **encryptionUpdate**, где **genericParameter** заполняется следующим образом:

– **parameterIdentifier**: в **standard** для обозначения смены ключа TGK MIKEY и обновления CSB на "уровне сессии" используется значение 0.

– **parameterValue** с сообщением MIKEY (I или R) в двоичном коде внутри **octetString**.

– **supersedes** не заполняется/не используется.

Для протокола MIKEY на "уровне сессии" **LogicalChannelNumber** не должно использоваться и может содержать любое значение.

RequestMode должно использовать **capabilityIdentifier** внутри **genericModeParameters ModeElement** следующим образом:

– **capabilityIdentifier** должно содержать в **standard** один из идентификаторов объекта MIKEY;

– **maxbitRate** и **collapsing** не используются;

– при функционировании протокола MIKEY на "уровне сессии" для определенного логического канала **nonCollapsing** используется со следующими значениями **GenericParameters**:

  • **parameterIdentifier**: для обозначения протокола MIKEY на "уровне сессии" в **standard** используется значение 0.

  • **parameterValue** с сообщением MIKEY (I или R) в двоичном коде внутри **octetString**.

  • **supersedes** не заполняется/не используется.

– **nonCollapsingRaw** не используется;

– **transport** (не используется или используется с заданными по умолчанию транспортными параметрами).

7.2 Функционирование протокола MIKEY на "уровне медиа"

Также протоколы управления ключами MIKEY могут функционировать на "уровне медиа"; т. е. TGK MIKEY применяется только к определенному логическому каналу в потоке медиа. Для реализации протокола MIKEY используется квитирование **TerminalCapability**, а для транспортировки закодированного сообщения MIKEY используется **OpenLogicalChannel/Ack**.

TerminalCapabilitySet должно использовать **h235SecurityCapability**, где **genericH235SecurityCapability** используется внутри **encryptionAuthenticationAndIntegrity** следующим образом:

– **capabilityIdentifier** должно содержать один из идентификаторов объекта MIKEY внутри **standard**;

– **maxbitRate**, **nonCollapsing** и **collapsing** не используются;

– **nonCollapsingRaw** не используется;

– **transport** (не используется или используется с заданными по умолчанию транспортными параметрами).

OpenLogicalChannel или **OpenLogicalChannelAck** должны использовать **genericParameter** внутри **encryptionSync** следующим образом:

– **parameterIdentifier**: в **standard** используется значение идентификатора параметра (см. таблицу 1), соответствующее реализуемому протоколу MIKEY;

– **parameterValue** с сообщением MIKEY (I или R) в двоичном коде в **octetString**;

– **supersedes** не заполняется/не используется;

– **synchFlag** в **encryptionSync** должен быть выставлен динамический номер полезной нагрузки. **h235key** не должно использоваться данной Рекомендацией и должно представлять собой пустую байтовую строку. **escrowentry** не используется.

MiscellaneousCommand должно использовать **encryptionUpdate**, где значение **genericParameter** внутри **encryptionSync** заполняется следующим образом:

– **parameterIdentifier**: в **standard** используется значение идентификатора параметра (см. таблицу 1), соответствующее реализуемому протоколу MIKEY;

– **parameterValue** с сообщением MIKEY (I или R) в двоичном коде в **octetString**;

– **supersedes** не заполняется/не используется.

RequestMode должно использовать **capabilityIdentifier** внутри **genericModeParameters ModeElement** следующим образом:

– **capabilityIdentifier** должно содержать один из идентификаторов объекта MIKEY внутри **standard**;

– **maxbitRate** и **collapsing** не используются;

– когда протокол MIKEY применяется на "уровне медиа" для определенного логического канала в **nonCollapsing** должны быть выставлены следующие параметры **GenericParameters**:

  • **parameterIdentifier**: в **standard** используется значение идентификатора параметра (см. таблицу 1), соответствующее реализуемому протоколу MIKEY.

  • **parameterValue** с сообщением MIKEY (I или R) в двоичном коде в **octetString**;

  • **supersedes** не заполняется/не используется.

– **nonCollapsingRaw** не используется;

– **transport** (не используется или используется с заданными по умолчанию транспортными параметрами).

7.3 Согласование возможностей MIKEY

Если протоколы MIKEY передаются при квитировании Terminal Capability Set/Request Mode и Open Logical Channel, протокол MIKEY в квитировании Open Logical Channel должен стать приоритетным и перезаписать предыдущую информацию по управлению ключами, приобретенную во время Terminal Capability Set/Request Mode.

Поскольку конечные точки могут не применять полный набор всех протоколов управления ключами MIKEY, или даже могут не применять ни одного из них (т. е. конечные точки потенциально не поддерживают данную Рекомендацию вообще), вызывающие конечные точки могут не знать о возможностях протокола MIKEY, поддерживаемых на вызываемых конечных точках. Поэтому

рекомендуется, чтобы информация о возможностях протокола управления ключами MIKEY согласовывалась с использованием квитирования Terminal Capability Set.

Во время окончательного/конечного согласования возможностей вызывающая конечная точка должна обозначить виды протокола MIKEY, поддерживаемые и принимаемые ею. Для этого вызывающая конечная точка должна обозначить возможности защиты протокола MIKEY, поддерживаемые ею. В **genericH235SecurityCapability** вызывающая конечная точка должна ввести значение идентификатора объекта в **capabilityIdentifier** (см. таблицу 1) согласно предпочитаемому профилю защиты и протоколу управления ключами MIKEY. Также поощряется предоставление других поддерживаемых протоколов MIKEY в порядке убывания приоритетности согласно политике защиты и ограничениям.

Вызываемая конечная точка, которая не поддерживает данную Рекомендацию, должна отклонить вызов, используя **ReleaseComplete** с **ReleaseCompleteReason** установленным в **securityDenied**, или может продолжить соединение незащищенной, если это допускается правилами политики защиты. Вызывающий может установить, что вызываемый не поддерживает запрашиваемые возможности MIKEY, изучив возвращенную возможность, которая не передает возможность MIKEY.

Вызываемая конечная точка, поддерживающая данную Рекомендацию, но не поддерживающая запрашиваемые возможности протокола MIKEY, должна обозначить поддерживаемые ею и приемлемые для нее протоколы MIKEY во время квитирования Terminal Capability Set.

Вызываемая конечная точка, которая поддерживает данную Рекомендацию и запрашиваемый протокол MIKEY, но не поддерживает особую комбинацию алгоритмов и параметров защиты MIKEY/SRTP (т. е. политику защиты MIKEY, SP), в качестве ответа должна вывести сообщение об ошибке (см. RFC 3830, пп. 5.1.1, 5.1.2 и 6.1.2). Вызываемой конечной точке следует включить поддерживаемую и приемлемую политику защиты MIKEY в алгоритмы и параметры защиты MIKEY/SRTP.

Для обеспечения защиты сообщений сигнализация вызова H.225.0 данная Рекомендация должна использовать туннелирование сообщений H.245 в сообщения Сигнализация вызова H.225.0. Данная Рекомендация может и не использовать туннелирование сообщения H.245, однако для обеспечения защиты сообщений H.245 требуется, чтобы, по крайней мере, использовалась безопасная передача с защитой целостности (TLS, IPsec). Этот вариант подробно в данной Рекомендации не рассматривается.

Предпочтительно, чтобы данная Рекомендация также использовала ускоренное соединение, где туннелированные сообщения H.245 инкапсулируются в сообщения сигнализация вызова H.225.0 Setup и CallProceeding-to-Connect. Это позволит завершить квитирование MIKEY в пределах не более двух проходов сообщения туда и обратно

Для защиты от атак понижения версии во время согласования возможностей конечная точка, подчиняющаяся данной спецификации, должна придерживаться процедуры, описанной в RFC 3830, пункт 6.15, где вызывающий составляет список предложенных идентификаторов протокола управления ключами MIKEY (KMID); см. RFC 4567, пункт 8.3, и включает этот список в общую полезную нагрузку расширения MIKEY каждого предложенного протокола MIKEY.

Для дуплексного канала значения протокола SRTP приписываются дважды, по одному разу в каждом направлении; а между конечными точками H.323 согласовывается только один динамический главный ключ MIKEY (TGK). Конечные точки приписывают значения направленным ключам сессии SRTP, применяя определенные идентификаторы криптосессии MIKEY к протоколам MIKEY и функции извлечения ключа SRTP.

8 Профиль защиты, использующий схему симметричного шифрования

В данном пункте описывается профиль защиты данной Рекомендации, в котором развертываются только симметричные методы шифрования.

На рисунке 3 изображен сценарий, в котором предполагается наличие общих секретов переход-переход (администрированных или конфигурированных) между объектами H.323 в домене H.323 (*sa, sb* и *sl*); таким образом делая возможным использование базового профиля защиты H.235.1 (аутентификация и/или целостность сообщения) протоколов RAS H.225.0 и сигнализации вызова. Для обеспечения аутентичности (т. е. целостности) сообщений сигнализации, которыми обмениваются конечные точки EP B и EP A, требуется, чтобы основной профиль защиты H.235.1 имел форму переход-переход.

Предполагается, что EP B синхронизирована по времени с другими конечными точками H.323 не жестко; в противном случае протокол MIKEY не сможет обеспечить безопасность.

ПРИМЕЧАНИЕ. – В данной Рекомендации не описываются какие-либо средства для надежной синхронизации времени среди объектов-участников. Обычно предполагается, что подобную синхронизацию времени можно достичь внутри корпоративных сетей.

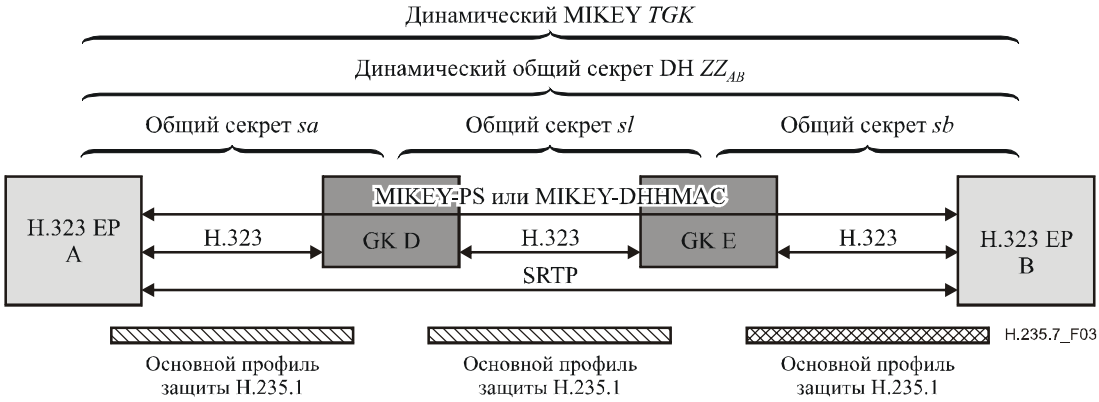

Рисунок 3/H.235.7 – Сценарий переход-переход только с общими секретами.

Основным принципом данного сценария является то, что протокол распределения ключей MIKEY-PS (симметричный, использующий предварительные общие секреты) или, если дело касается совершенной передовой секретности, протокол согласования ключей MIKEY-DHHMAC (алгоритм Диффи-Хеллмана, использующий HMAC) используется внутри домена H.323. RFC 4650 предлагается в качестве дополнения к MIKEY, см. Дополнение I.

Для EP B (инициатор MIKEY), вызывающей EP A (ответчик MIKEY), между конечными точками EP A и EP B создается динамический общий секрет ZZAB как часть RAS H.225.0 и Setup для вызова. Динамический общий секрет ZZAB далее используется в качестве предварительного общего секрета MIKEY, из которого протокол MIKEY образует симметричный шифр и ключи аутентификации на конечных точках EP A и EP (на рисунке не показано).

Вызывающая конечная точка EP B генерирует TGK MIKEY (в действительности это главный ключ) для EP A. EP B создает сообщения протокола MIKEY и инкапсулирует все сообщение MIKEY в контейнер внутри туннелированного сообщения **TerminalCapabilitySet/OpenLogicalChannel**. Привратник GK E в сетевом окружении, маршрутизируемом привратником, просто направит контейнер MIKEY другой конечной точке A без декодирования самого MIKEY. EP A завершает протокол MIKEY в домене H.323.

Таким образом, конечные точки EP B и EP A создают *TGK*.

Протокол MIKEY-PS или MIKEY-DHHMAC передаются от EP B к EP A. Таким образом, конечные точки получают *TGK* и могут образовывать ключи сессии SRTP/SRTCP. Протоколы SRTP и SRTCP применяют эти ключи сессии на сквозной основе.

ПРИМЕЧАНИЕ 1. – Протокол MIKEY обеспечивает протокол SRTP всеми необходимыми параметрами (алгоритмы, длина ключа, время существования и т. д.) в качестве части реализуемой политики MIKEY.

Привратники не принимают активного участия в обработке протокола MIKEY и выступают в качестве хранилища и направляющего реле для инкапсулированных сообщений MIKEY.

Для установления вызова со стороны EP A процедура выполняется аналогично, но в обратном направлении, при этом EP A является инициатором, а EP B – ответчиком.

ПРИМЕЧАНИЕ 2. – Сценарий, изображенный на рисунке 3, также поддерживает модель прямой сигнализации вызова, не маршрутизируемую привратником(ами). В таком окружении, маршрутизируемом напрямую, пересылка сообщений сигнализации вызова H.225.0 (Setup и т. д.) осуществляется на сквозной основе внутри домена H.323 и не маршрутизируется привратником. См. Дополнение II для иллюстрации использования H.235.4 для этих целей.

ПРИМЕЧАНИЕ 3. – Протокол MIKEY использует штампы времени в протоколе защиты в качестве средства обеспечения защиты сообщения управления ключами от воспроизведения (replay). Для этого требуется, чтобы часы на конечных точках были не жестко синхронизированы по времени (в допустимых пределах расхождения по времени). Считается, что такой синхронизации времени можно достичь при использовании настроенных вручную таймеров/часов или некоторых протоколов синхронизации сетевого времени (например, NTP RFC 1305). Как таковая, синхронизация времени в домене H.323 должна подходить, по крайней мере, для корпоративных сетей, см. также RFC 3830, пункты 5.4 и 9.3.

ПРИМЕЧАНИЕ 4. – Применение быстрого старта и раннее включение мультимедиа (ранний запуск) (early media) совместно с протоколом MIKEY-DHHMAC не рекомендуется. Если применение быстрого старта и раннего включения мультимедиа необходимо, конечные точки должны вместо протокола MIKEY-DHHMAC использовать протокол MIKEY-PS.

ПРИМЕЧАНИЕ 5. – Особым случаем изображенного сценария с несколькими привратниками является сценарий с одним привратником. В таком случае использование LRQ/LCF на удаленном привратнике/конечной точке не обязательно.

Следующее обеспечивает более детализированные потоки сообщений сценария на рисунке 3. Данный сценарий предполагает наличие одного или более маршрутизирующих привратников в домене H.323, где сообщения H.245 туннелируются в H.225.0, и применяется быстрый старт.

ПРИМЕЧАНИЕ 6. – Схемы прохождения сообщений также охватывают случай прямого соединения (без маршрутизирующих привратников), где обмен сообщениями сигнализации вызова H.225.0 между конечными точками происходит напрямую и не маршрутизируется привратниками, см. Дополнение II.

С помощью процедуры, описываемой в данном пункте, между конечными точками H.323 EP A и EP во время этапа 1 с использованием согласования ключей Диффи-Хеллмана создается сквозной общий секрет ZZ_{AB}. Данное согласование ключей Диффи-Хеллмана возникает во время фазы регистрации и допуска RAS H.225.0 и, в случае с несколькими привратниками, во время обмена сообщениями **LRQ/LCF** между привратниками. Генерируемый общий секрет Диффи-Хеллмана служит в качестве ключа сквозной аутентификации и действует в течение вызова. Протокол MIKEY-PS (или MIKEY-DHHMAC) возникает во время этапа 2 установления вызова отдельно и создает секреты на основе вызова MIKEY для канала-носителя.

В Дополнении II описывается альтернативная дополнительная процедура использования процедуры DRC1 H.235.4, для того чтобы разрешить привратнику генерировать и распределять общий секрет конечным точкам EP A и EP B.

В схеме на рисунке 4 показан основной профиль защиты H.235.1, в котором каждое сообщение защищено полностью (аутентификация и целостность). Кроме того, сообщение проходит подобный путь, когда применяется опция "только аутентификация" основного профиля защиты (на рисунке не показано). В этом случае значение HMAC вычисляется не по всему сообщению, а только по подмножеству (ClearToken в CryptoToken) сообщения RAS/H.225.0.

В примере (см. рисунок 4) EP B (инициатор MIKEY) вызывает EP A (ответчик MIKEY), используя ускоренный старт. Сначала конечные точки H.323 A и B регистрируются на привратнике, используя RRQ, и предоставляют свои половины ключа DH (ga и gb). Для передачи половины ключа DH во время RRQ и ACF следует использовать ClearToken (в CryptoHashedToken). По этой причине не следует использовать поле challenge.

Половину ключа DH следует передавать в dhkey как часть ClearToken. В ClearToken вместо идентификатора объекта "T", показывающего на то, что данный профиль защиты используется совместно с основным профилем H.235.1, должен быть указан идентификатор объекта "TG" (см. 8.5). Привратник должен сохранять каждую половину ключа пока происходит регистрация конечной точки. При использовании подтверждения активности (keep-alives) или упрощенной перерегистрации (re-RRQ) конечные точки не должны включать половины ключа DH. Для обозначения того, что привратник поддерживает данный профиль защиты, RCF должен использовать идентификатор объекта "TG" OID в ClearToken.

EP B, пытающаяся установить соединение с EP A, запрашивает допуск у привратника D (ARQ). В сообщении ARQ следует использовать идентификатор объекта "TG" в ClearToken. Также идентификатор объекта OID "TG" должен использоваться в ClearToken всех сообщений RAS.

Сценарий охватывает многочисленных, сцепленных привратников, но может равным образом поддерживать и единственного привратника. Обнаружение удаленной конечной точки должно быть выполнено в соответствии с 8.1.6/H.323 "Дополнительная сигнализация вызываемой конечной точки" с использованием **LRQ/LCF**. Так инициирующая конечная точка определяет местонахождение зоны удаленного привратника и таким образом получает половину ключа DH вызываемой конечной точки.

Если привратнику GK E необходимо определить местонахождение зоны удаленного привратника, GK E должен послать сообщение **LRQ**. В случае многоадресной передачи **generalID** в CryptoToken сообщения **LRQ** не используется. Если GK D не поддерживает данный профиль, он должен ответить сообщением **LRJ**. В противном случае GK D должен ответить сообщением **LCF**, которое включает половину ключа DH конечной точки EP A. Затем GK E должен ответить сообщением **ACF**, включающим половину ключа DH конечной точки EP A. Если GK E не удалось определить местонахождение удаленной конечной точки A, он отвечает сообщением **ARJ**.

Связь между двумя привратниками должна быть защищена в соответствии с H.235.1. Предполагается, что для этого доступен общий секрет *sl*. Поскольку сообщение **LRQ** среди привратников обычно является многоадресным, общий секрет *sl* обычно в действительности представляет собой не пару общих секретов, а группу общих секретов внутри потенциального скопления привратников. Данное предположение ограничивает масштабируемость в общем случае и не обеспечивает аутентификацию источника. Между тем, считается, что в корпоративных сетях с ограниченным небольшим числом проверенных привратников, подобные ограничения допустимы. Обеспечение защиты многоадресного взаимодействия между привратниками при помощи электронной подписи могло бы преодолеть данные ограничения; это, однако, остается предметом дальнейших исследований.

EP B получает половину ключа DH конечной точки EP A (**ACF**). Сообщение **ACF** должно содержать ключ DH вызываемой конечной точки в **dhkey** в основном **ClearToken** H.235.1, но значение идентификатора объекта OID должно быть "TG" вместо "T". Все остальные поля внутри **ClearToken** не должны подвергаться изменению данным профилем защиты.

ПРИМЕЧАНИЕ 7. – Конечные точки оперируют с половинами ключа DH, который остается статичным все время регистрации для всех вызовов. Это, однако, не является недостатком защиты, поскольку каждая конечная точка применяет половины ключа, выбранные случайным образом.

Тем не менее, конечные точки должны вводить новое случайное значение в 512 бит (т. е. 64 байта) в **challenge** наряду со своей половиной ключа DH, (см. RFC 2631, пункт 2.3). Данные значения **challenge** зависят от вызова и вносят необходимую произвольность и своевременность в генерирование ключа DH.

Затем исходящая конечная точка EP B может вычислить g^{ab} и динамический общий секрет ZZAB, используя случайное значение в **challenge** и результат, полученный от MIKEY-PRF(g^{ab}, 0x12F905FE || **challenge**) (см. RFC 3830, пункты 4.1.2–4.1.4). Затем протокол MIKEY может вычислить шифрование/код (Me) и ключи аутентификации (Ma), используя протокол MIKEY-PRF (см. RFC 3830, пункты 4.1.2–4.1.4).

Во время этапа 2, исходящая конечная точка EP B должна вычислить новое значение MIKEY *TGK*, а затем создать сообщение MIKEY I_message Imsg согласно протоколу MIKEY-PS, используя *Me* и *Ma*; также из *TGK* следует вычислить ключи сессии SRTP, как описано в RFC 3711, пункт 4.3 (на рисунке не показано).

Необходимо перевести сообщение MIKEY I_message в двоичный код.

Исходящей конечной точке EP B всегда следует включать свою половину ключа DH в **dhkey** **ClearToken**, таким образом делая возможной модель прямого соединения, поддерживаемую привратником. Следует включить **ClearToken** в сообщение Setup и переслать его EP A. Маршрутизирующий привратник должен направить передаваемое **ClearToken** на следующий переход (без внесения изменений в сообщение MIKEY).

Затем получающая конечная точка EP A вычисляет g^{ab} и динамический общий секрет ZZAB из MIKEY-PRF(g^{ab}, 0x12F905FE || **challenge**) (см. RFC 3830, пункты 4.1.2–4.1.4). Затем протокол MIKEY вычисляет код (*Me*) и ключи аутентификации (*Ma*), используя протокол MIKEY-PRF (см. RFC 3830, пункты 4.1.2–4.1.4). Затем передаваемые TGK могут быть возвращены.

Затем из *TGK* принимающая конечная точка EP A может вычислить ключи сессии SRTP, как описано в RFC 3711, пункт 4.3 (на рисунках не показано).

EP A может создать аналогичное сообщение R_message Rmsg, но должна сделать это, только по запросу EP B или при необходимости (DH). Сообщение R_message передается внутри сообщения CallProceeding-to-Connect (CP/C).

Сообщение CallProceeding-to-Connect (CP/C) посылается EP B.

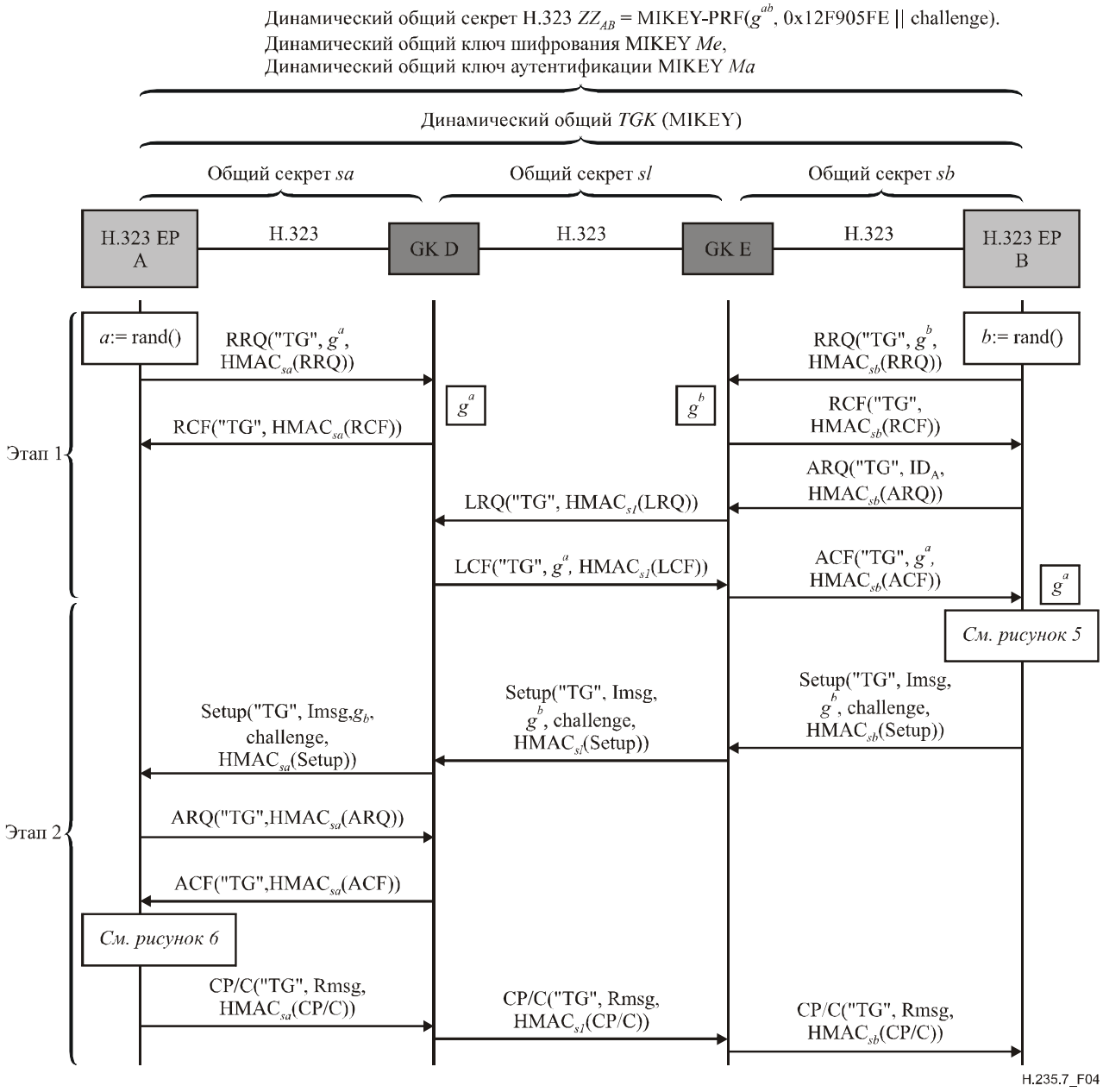

Рисунок 4/H.235.7 – Пример: конечная точка B вызывает конечную точку A (маршрутизируемую привратником GK) с предварительным общим секретом MIKEY

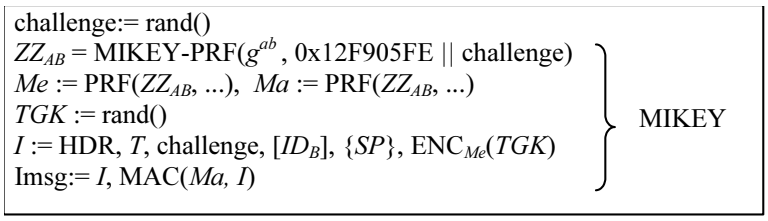

Рисунок 5/H.235.7 – Обработка предварительного общего секрета MIKEY конечной точкой EP B

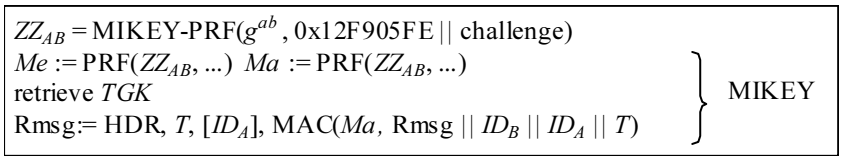

Рисунок 6/H.235.7 – Обработка предварительного общего секрета MIKEY конечной точкой EP A

8.1 Завершение вызова H.323

Поскольку взаимодействующие конечные точки сохраняют состояние для MIKEY и SRTP, необходима подходящая процедура завершения. На рисунке 7 приводится пример прохождения сообщений в случае, когда конечная точка EP B (инициатор MIKEY) завершает вызов. В основном поток проходит согласно 8.5/H.323 "Фаза E – Завершение вызова".

ПРИМЕЧАНИЕ. – На рисунке 7 также показаны дополнительные процедуры отключения для случая, когда конечные точки полностью отменяют регистрацию. Затем конечные точки должны удалить частные ключи DH (*a* или *b*) и открытую половину ключа DH (g^a или g^b).

Поскольку процедура завершения вызова не зависит от данного профиля защиты, могут быть использованы любые применимые идентификаторы объекта основного профиля (H.235.1, H.235.3 и т. д.), На рисунке 7, однако, не показаны какие-либо идентификаторы объекта.

Если конечная точка снова регистрируется на привратнике, необходимо вычислить новые половины ключа DH. Однако для завершения вызова в любом случае нет необходимости в полной отмене регистрации. Если конечная точка решает остаться зарегистрированной на привратнике, можно продолжить использовать статические половины ключа DH.

В случае, если конечные точки остаются зарегистрированными и процедура разрыва соединения не применяется, конечные точки должны удалить только информацию о вызове, включая половину ключа DH, **challenge**, ключи MIKEY *Me*, *Ma*, *TGK* и связанную информацию о SRTP.

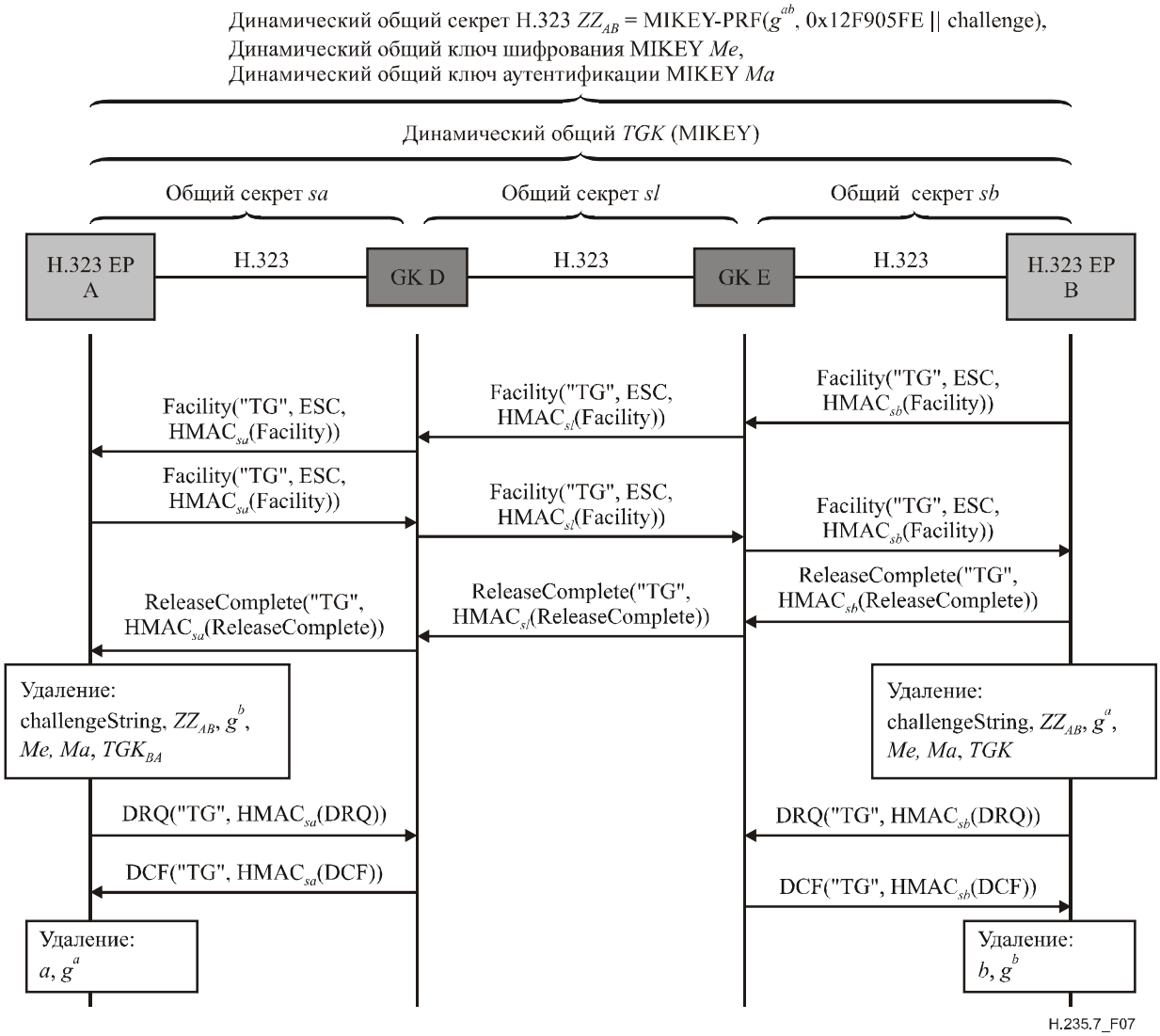

Рисунок 7/H.235.7 – Пример: конечная точка B завершает вызов

8.2 Смена ключей шифрования TGK и обновление CSB

Протокол MIKEY имеет встроенную поддержку смены ключей шифрования TGK и/или обновления информации CSB. Профиль данной Рекомендации должен использовать для этой цели процедуру MIKEY-PS в RFC 3830, пункт 4.5, или, если дело касается совершенной передовой секретности, RFC 4650, пункт 3.1, которая позволяет обновить TGK до окончания срока действия, или обновить другую информацию, не внося изменений в TGK.

Механизм смены ключей шифрования TGK и обновления CSB полезен для обеспечения защиты связки (группы) логических каналов в рамках одной политики защиты. Для этого рекомендуется выполнять протокол MIKEY с предварительными общими секретами полностью, как описано в пункте 8, только для первого логического канала. Все последующие логические каналы, которые должны выполнять одну и ту же политику защиты MIKEY или один и тот же TGK, должны использовать механизм обновления CSB без механизма смены ключей шифрования в данном пункте, делая ссылку на первоначальный идентификатор CSB-ID и пропуская обновленные данные TGK. Это позволяет настроить логические каналы или крипто сессии MIKEY эффективнее, чем при запуске полного протокола MIKEY на каждом логическом канале.

Сообщения смены ключа шифрования TGK MIKEY или обновления CSB должны быть инкапсулированы и переданы в **MiscellaneousCommand** внутри сообщения Facility. Значение **tokenOID ClearToken** должно быть выставлено на "TG".

Если протокол MIKEY запущен на "уровне медиа", конечная точка EP B определяет, на каком логическом канале будет применяться смена ключей шифрования TGK и/или обновление CSB. Конечная точка EP A, будучи ответчиком, также будет использовать **MiscellaneousCommand** в сообщении Facility для передачи MIKEY R_message (при наличии).

Для смены ключей шифрования TGK (см. рисунок 8), конечная точка EP B, будучи инициатором MIKEY, должна сгенерировать новый TGK.

EP A, будучи ответчиком, может подтвердить полученное сообщение о смене ключей шифрования TGK, если этого требует конечная точка EP B. Конечная точка EP A создает аналогичные сообщения R_messages. Конечная точка EP B посылает сообщение R_message внутри сообщения Facility на конечную точку EP A.

Для обновления CSB, процедура аналогична за исключением того, что сообщение MIKEY не должно содержать TGK.

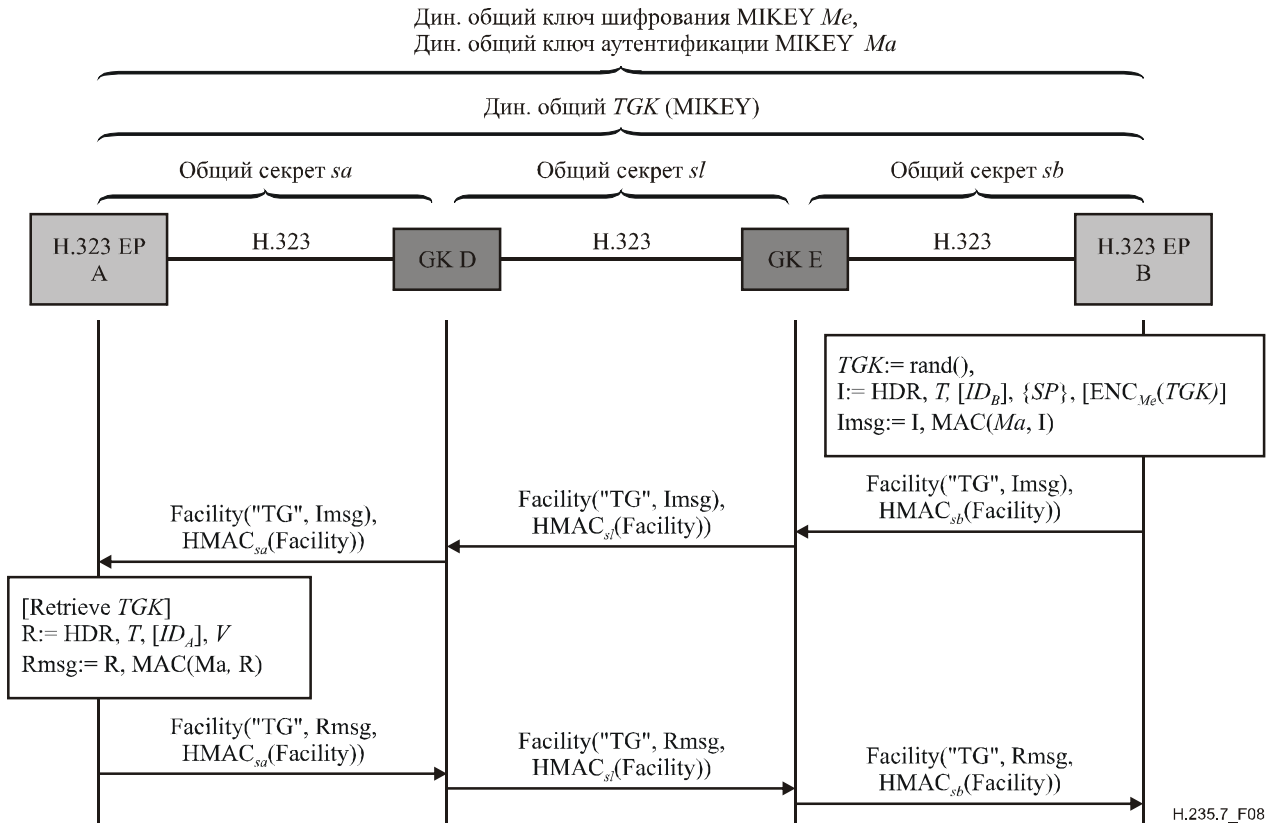

Рисунок 8/H.235.7 – Пример: конечная точка B обновляет шифровальный ключ

ПРИМЕЧАНИЕ. – Подтверждающее сообщение Facility от EP A к EP B является дополнительной возможностью и необходимо только в тех случаях, когда EP B также запрашивает верификационное сообщение (MIKEY R_message), используя флажок V в MIKEY HDR.

В данной Рекомендации не определяются процедуры для смены ключей шифрования TGK и/или обновления CSB, осуществляемых ответчиком; это является предметом дальнейшего исследования.

8.3 Поддержка туннелирования H.245

Если во время сеанса необходимо добавить логические каналы, следует использовать режим туннелирования H.245, при котором туннелированные сообщения H.245 передаются внутри сообщения Facility.

8.4 Алгоритмы SRTP

Данный профиль защиты должен использовать укороченный (алгоритм) HMAC-SHA1-32 с длиной метки аутентификации *n_tag* равной 32 битам в качестве заданного по умолчанию алгоритма аутентификации для RTP. Другие длины меток аутентификации, определенные RFC 3711, также должны поддерживаться и согласовываться через параметр политики защиты MIKEY (SP) как приемлемые.

8.5 Список идентификаторов объекта

"TG"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 70}	Обозначает **ClearToken** основного уровня для H.235.1 в рамках данной Рекомендации. Данный OID также означает, что для вычисления общего секрета ZZ_{AB} используется протокол MIKEY-PRF.

9 Профиль защиты, использующий схему ассиметричного шифрования

В данном пункте описан профиль защиты данной Рекомендации, который развертывает асимметричные методы шифрования. Данный сценарий обеспечивает наибольшую масштабируемость.

Существование промежуточных объектов (т. е. привратников), которые могут перехватить TGK MIKEY и/или ключи сессии SRTP, может быть не всегда приемлемым. На рисунке 9 изображен сценарий, реализующий инфраструктуру открытых ключей (PKI) для создания медиа ключей SRTP полностью на сквозной основе.

Допущение: предполагается, что EP A и EP B располагают частным ключом (*SK*), а также сертифицированным открытым ключом (*cert*). Тем не менее, EP A и GK E, а также EP B и GK D могут совместно использовать (администрированные/конфигурированные) общие секреты в случае, когда защита сообщений RAS H.225.0 и сигнализации вызова обеспечивается с использованием H.235.1. Кроме того, предполагается, что EP A и EP B синхронизированы по времени не жестко, в противном случае протокол MIKEY не сможет обеспечивать защиту.

Аутентификации/целостности сообщения можно достичь, либо используя предварительно конфигурированные общие секреты переход-переход (*sa, sb* и *sl*) и базовый профиль защиты H.235.1, либо, в более общем случае, используя PKI для создания динамических общих секретов со гибридным профилем защиты H.235.3.

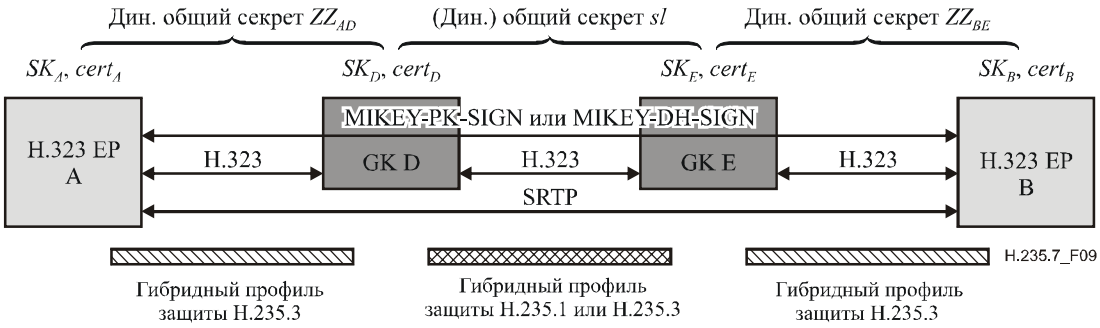

Рисунок 9/H.235.7 – Сценарий сквозной передачи с использованием PKI (многочисленные GK)

EP A и EP B запускают протоколы MIKEY-PK-SIGN или MIKEY-DH-SIGN на сквозной основе и таким образом создают MIKEY TGK, на основе которой оконечные системы вычисляют ключи сессии SRTP.

ПРИМЕЧАНИЕ 1. – Протокол MIKEY-PK-SIGN удовлетворяет требованиям управления ключами на основе RSA.

ПРИМЕЧАНИЕ 2. – При использовании методов PKI более общее окружение H.323, включающее в себя многочисленных сцепленных привратников в ряд, определенно охвачено лучше, чем менее масштабируемые и ограниченные архитектуры, использующие симметричные методы шифрования.

ПРИМЕЧАНИЕ 3. – Не рекомендуется совмещение быстрого старта и раннего включения мультимедиа с протоколом MIKEY-DH-SIGN. Если применение быстрого страта и раннего включения мультимедиа необходимо, конечные точки должны использовать не MIKEY-DH-SIGN, а MIKEY-PK-SIGN.

Ниже приводится более детальная иллюстрация прохождения сообщений по сценарию на рисунке 9. В данном сценарии внутри домена H.323 присутствуют многочисленные привратники.

В нижеследующих рисунках предполагается наличие маршрутизирующего привратника (модель, маршрутизируемая привратником), где сообщения H.245 туннелируются в H.225.0 (Fast start).

ПРИМЕЧАНИЕ 4. – На схеме прохождения также показан случай прямого прохождения (без маршрутизирующего привратника), где обмен сообщениями сигнализации вызова H.225.0 происходит между конечными точками напрямую и не направляется каким-либо привратником.

На схеме также показан гибридный профиль защиты H.235.3, где первоначальные сообщения RAS защищаются полностью (аутентификация и целостность) с использованием цифровых подписей и дополнительных сертификатов. Он предназначен для создания динамических общих секретов ZZ_{BE} и ZZ_{AD} между конечными точками и привратником на следующем переходе, таким образом делая статические общие секреты излишними. Кроме того, сообщение проходит аналогичный путь при применении опции "только аутентификация" профиля защищенной цифровой подписи (на рисунке не показано).

В примере прохождения сообщений EP B (инициатор MIKEY) вызывает EP A (ответчик MIKEY) (см. рисунок 10).

Во время этапа 1 конечные точки H.323 выполняют первичную регистрацию на привратнике следующего перехода и предоставляют свои половины ключа DH(g^a и g^b).

EP B, пытающаяся установить соединение с EP A, запрашивает допуск у привратника E. В случае, если информация о сертификате еще не доступна EP, EP B может запросить сертификат *certC*, включив элемент профиля защиты в **ClearToken.** Данный элемент профиля защиты должен использовать следующие поля:

– **elementID** со значением 7, обозначающим элемент запроса сертификата (certificate request element); На рисунке 10 это обозначено надписью "certFlag";

– **paramS** не используется;

– **element** содержит Element, где выставлено значение **flag** – TRUE.

Безопасность сообщения ARQ и всех последующих сообщений RAS и Сигнализации вызова H.225.0 обеспечивается динамическим общим секретом ZZ_{BE} с использованием базового профиля защиты H.235.1. В случае, когда EP B запрашивает поиск сертификата, GK E извлекает certC из местного или какого-либо другого хранилища сертификатов и передает результат как часть сообщения ACF в **certificate ClearToken** и включает элемент профиля защиты. Данный элемент профиля защиты должен использовать следующие поля:

– elementID со значением 8, обозначающим элемент ответа сертификата; на рисунке 10 это обозначено надписью "certFlag";

– **paramS** не используется;

– **element** содержит Element, где выставлено значение **flag** – TRUE.

В случае, когда привратник получает многочисленные сертификаты для соответствующей конечной точки/UA, сообщение ACF в действительности будет содержать несколько ClearToken, каждое из которых будет передавать отдельный сертификат в **certificate**. Затем конечная точка выбирает подходящий сертификат. Тем не менее, может случиться так, что поиск сертификата занимает слишком много времени; например, при контакте с внешними хранилищами сертификатов. Если привратнику не удается предоставить сертификат(ы) вовремя, или не удается предоставить их вообще, сообщение ACF возвращается с пустым **certificate** в ClearToken, которое содержит элемент профиля защиты, в котором:

– **elementID** со значением 8, обозначающим элемент ответа сертификата;

– **paramS** не используется;

– **element** содержит Element, где выставлено значение **flag** – FALSE.

Задачей конечной точки затем является прекращение и попытка определить местонахождение подходящего сертификата средствами, не описанными в данной Рекомендации. В случае, если привратнику удается получить сертификат, превысив необходимое время ответа, привратник должен обозначить данную ситуацию, оставив **certificate** пустым и включив элемент профиля защиты в ClearToken, где:

– **elementID** со значением 8, обозначающим элемент ответа сертификата;

– **paramS** не используется;

– **element** содержит Element, где выставлено значение **flag** – TRUE.

В этом случае привратник должен возвратить ClearToken в сообщении ACF.

Во время этапа 2 исходящая EP B (инициатор MIKEY) может генерировать новый MIKEY TGK и вычислить соответствующее сообщение MIKEY I_message Imsg, применив протокол управления ключами MIKEY-PK-SIGN (см. рисунки 11 и 12); или, если дело касается совершенной передовой секретности, протокол согласования ключей MIKEY-DH-SIGN (DH, использующий цифровые подписи). В качестве опции предлагается протокол MIKEY-DH-SIGN.

Ключи сессии SRTP могут быть вычислены из TGK, как описано в RFC 3711, пункт 4.3 (на рисунках не показано).

ПРИМЕЧАНИЕ 5. – На рисунках 11 и 12 не показаны все подробности MIKEY, некоторые части на рисунке не показаны.

Сообщение MIKEY I_message кодируется в двоичном коде и инкапсулируется в H.245 **OpenLogicalChannel**.

ClearToken включается в сообщение Setup и посылается на EP A. Маршрутизирующий привратник направляет передаваемое сообщение MIKEY I_message на следующий переход (без внесения изменений сообщения MIKEY).

В случае многочисленных маршрутизирующих привратников, защита передачи сообщения сигнализации вызова между привратниками может быть обеспечена при применении администрированного общего секрета и использовании H.235.1 или H.235.3 и частных/открытых ключей.

Затем EP A может вычислить ключи сессии SRTP из *TGK*, как описано в RFC 3711, пункт 4.3 (на рисунках не показано).

Будучи ответчиком MIKEY, EP A может транслировать/компилировать сообщение MIKEY R_message Rmsg, используя ключ MIKEY *Ma*, и включать сообщение MIKEY R_message в сообщение CallProceeding-to-Connect (CP/C).

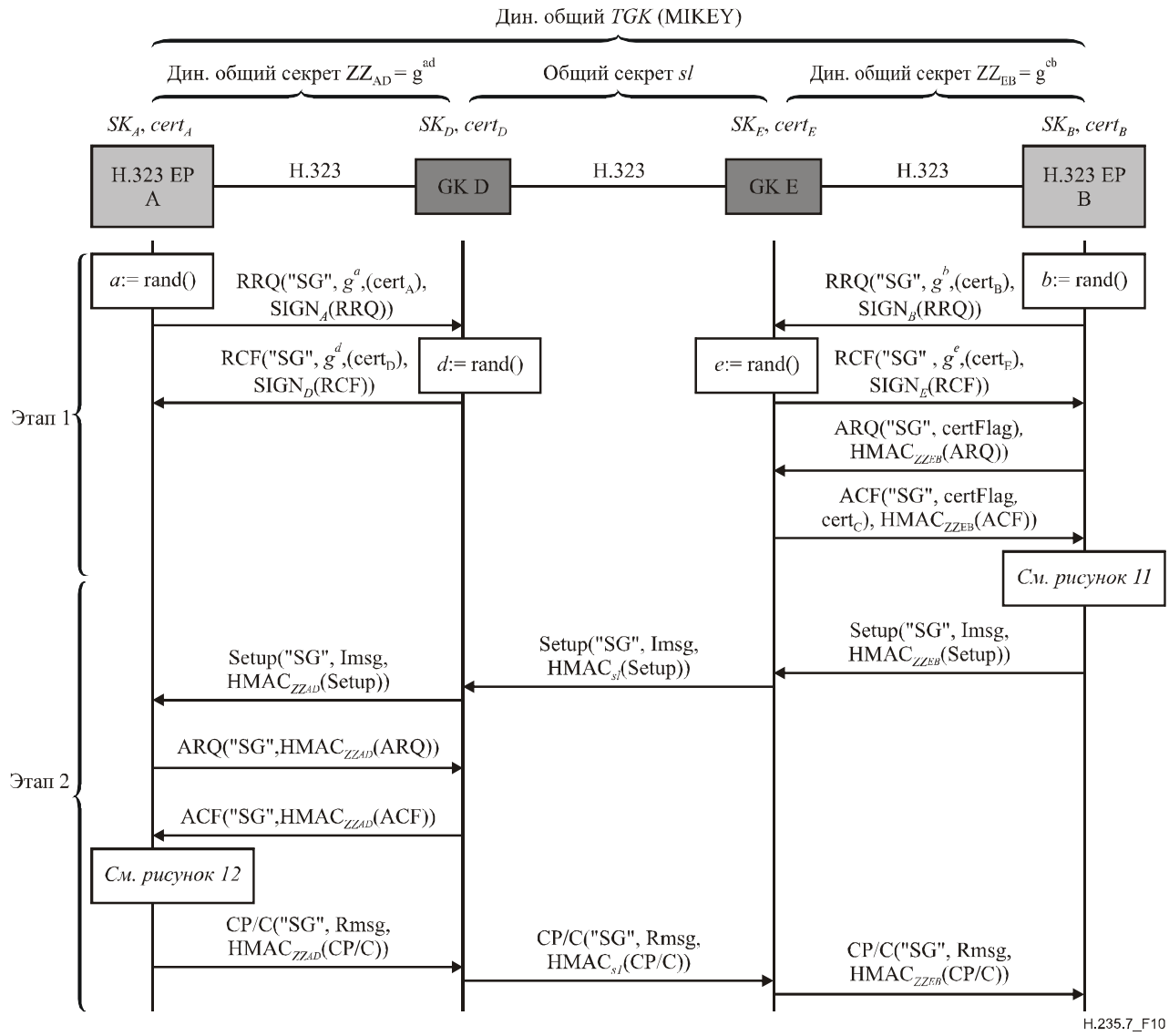

Рисунок 10/H.235.7 – Пример: EP B вызывает EP A (модель с маршрутизацией многочисленными привратниками) с MIKEY-PK-SIGN

TGK:= rand()
env-key:= rand()
Me, Ma:= PRF(env-key,…|| Rand)
PKE:= ENC_{PK-A}(env-key,…|| Rand)
K:= ENC_{Me}(ID_B || [*TGK*])
KEMAC:= ENC_{Me}(ID_B || [*TGK*])
M:= HMAC-SHA1(Ma, K)
I:= HDR, *T*, rand(), [ID_B | $Cert_B$], {*SP*}, [chash], *KEMAC*, *PKE*
Imsg:= *I*, $Sign_{SK-B}$(*I*)

Рисунок 11/H.235.7 – Обработка MIKEY-PK-SIGN конечной точкой EP B

Retrieve env-key, TGK
Ma:= PRF(env-key,…|| Rand),
Rmsg:= HDR, *T*, [ID_A], HMAC-SHA1(Ma, Rmsg || ID_A || ID_B || *T*)

Рисунок 12/H.235.7 – Обработка MIKEY-PK-SIGN конечной точкой EP A

Частным случаем изображенного сценария с многочисленными привратниками является сценарий с одним привратником. В таком случае, при обнаружении удаленного привратника/конечной точки обязательно используется LRQ/LCF.

9.1 Завершение вызова H.323

Поскольку вовлеченные конечные точки поддерживают состояние для MIKEY и SRTP, необходима подходящая процедура завершения. На рисунке 13 изображен пример прохождения сообщений в случае, когда EP B (инициатор MIKEY) завершает вызов. В основном, поток проходит согласно 8.5/H.323 "Фаза E – Завершение вызова".

ПРИМЕЧАНИЕ. – На рисунке 13 также показаны дополнительные процедуры разрыва соединения в случае, когда конечные точки полностью отменяют регистрацию. Затем конечные точки должны удалить частный ключ DH (*a* или *b*) и половину открытого ключа DH (g^a или g^b).

Поскольку процедура завершения вызова не зависит от данного профиля защиты, может использоваться любой применимый OID лежащего в основе профиля защиты; поэтому на рисунке 13 OID не изображены.

Если конечная точка снова регистрируется на привратнике, должны быть сгенерированы новые половины ключа DH. Однако только для завершения вызова нет необходимости в полной отмене регистрации. Если конечная точка решает остаться зарегистрированной на привратнике, могут продолжать использоваться статические половины ключа DH.

В случае, когда конечные точки остаются зарегистрированными, и процедура разрыва соединения не применяется, конечные точки должны удалить только информацию, касающуюся вызова, включая соответствующую половину ключа DH, **challenge**, ключи MIKEY *Me*, *Ma*, *TGK* и информацию, касающуюся сессии SRTP.

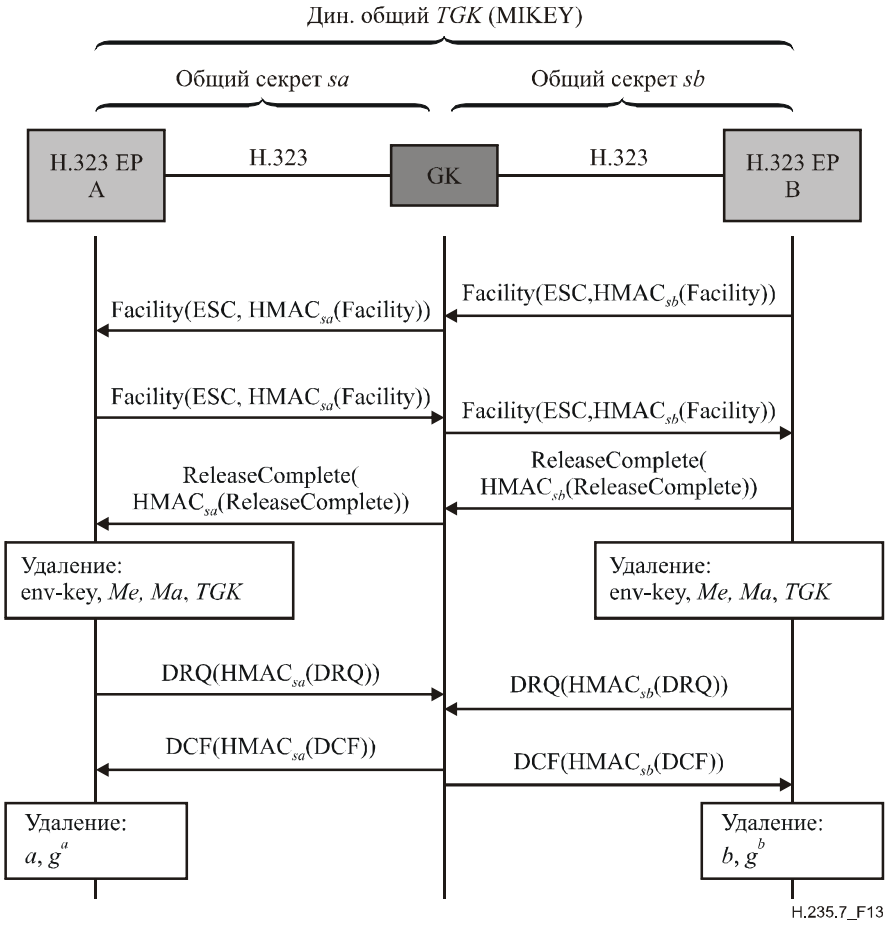

Рисунок 13/H.235.7 – Пример: конечная точка B завершает вызов

9.2 Смена ключа шифрования TGK и обновление CSB

Протокол MIKEY имеет встроенную поддержку смены ключей шифрования TGK и/или обновления информации CSB. Профиль данной Рекомендации должен использовать для этой цели процедуру MIKEY-PK-SIGN в RFC 3830, пункт 4.5, которая позволяет обновить TGK до окончания срока действия, или обновить другую информацию(CSB), не внося изменений в TGK.

Механизм смены ключей шифрования TGK и обновления CSB полезен для обеспечения защиты пакета логических каналов в рамках одной политики защиты. Для этого рекомендуется выполнять/запускать (полный) протокол MIKEY-PK-SIGN, как описано в пункте 8, только для первого логического канала. Все последующие логические каналы, которые должны применять одну и ту же политику защиты MIKEY или один и тот же TGK, должны использовать механизм обновления CSB без механизма смены ключей шифрования в данном пункте, делая ссылку на первоначальный идентификатор CSB-ID и пропуская обновленные данные TGK. Это позволяет настроить логические каналы или крипто сессии MIKEY эффективнее, чем при запуске полного протокола MIKEY на каждом логическом канале.

Сообщения смены ключа шифрования TGK MIKEY или обновления CSB должны быть включены в **MiscellaneousCommand** внутри сообщения Facility message. Значение **tokenOID ClearToken** должно быть выставлено на "SG".

Если протокол MIKEY запущен на "уровне медиа", конечная точка EP B определяет на каком логическом канале будет применяться смена ключей шифрования TGK и/или обновление CSB. EP A, будучи ответчиком, также будет использовать **MiscellaneousCommand** в сообщении Facility для передачи MIKEY R_message (при наличии).

Для смены ключей шифрования TGK (см. рисунок 14), конечная точка EP B, будучи инициатором MIKEY, должна сгенерировать новый TGK. **mikey** должно содержать соответствующее сообщение MIKEY I_message.

Ответчик (EP A) может подтвердить полученное сообщение о смене шифровальных ключей TGK, если этого требует конечная точка EP B. EP A создает аналогичное сообщение R_messages. Сообщение R_message передается внутри сообщения Facility. Rmsg является соответствующим сообщением ответа MIKEY, передаваемом в **octetString GenericParameter**. EP A посылает сообщение Facility на EP B.

Для обновления CSB, инициированного инициатором, процедура аналогична, за исключением того, что сообщение MIKEY не должно содержать TGK (см. рисунок 14).

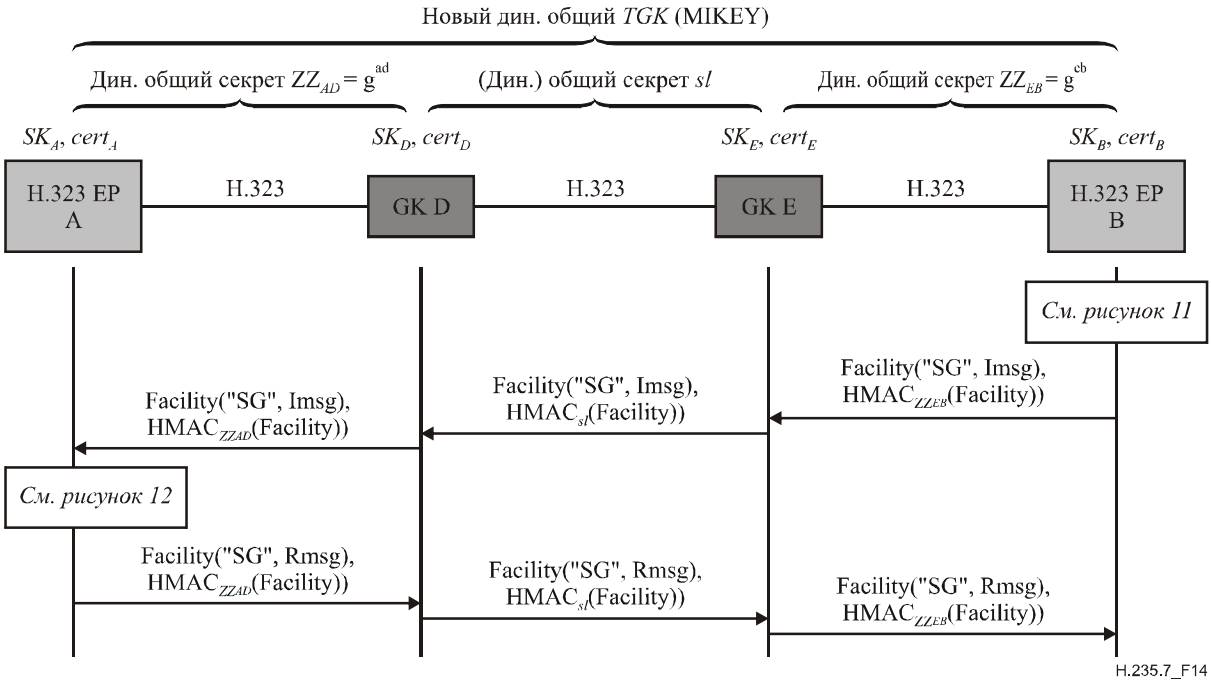

Рисунок 14/H.235.7 – Пример:EP B (инициатор) инициирует смену шифровальных ключей TGK и обновление ключей

ПРИМЕЧАНИЕ. – Подтверждающее сообщение Facility от EP A к EP B является дополнительной возможностью и необходимо только в тех случаях, когда EP B также запрашивает верификационное сообщение (MIKEY R_message), используя флажок V в MIKEY HDR.

В данной Рекомендации не определяются процедуры для смены ключей шифрования TGK и/или обновления CSB, инициируемых ответчиком; это является предметом дальнейшего исследования.

9.3 Поддержка туннелирования H.245

Если во время сеанса необходимо добавить логические каналы, следует использовать режим туннелирования H.245, при котором туннелированные сообщения H.245 передаются внутри сообщения Facility.

9.4 Алгоритмы SRTP

Данный профиль защиты должен использовать укороченный (алгоритм) HMAC-SHA1-32 с длиной метки аутентификации *n_tag* равной 32 битам в качестве заданного по умолчанию алгоритма аутентификации для RTP. Также должны поддерживаться и согласовываться через параметр политики защиты MIKEY (SP) как приемлемые другие длины меток аутентификации, определенные RFC 3711.

9.5 Список идентификаторов объекта

"SG"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 71}	Обозначает ClearToken основного уровня для H.235.3 в рамках данной Рекомендации.

Дополнение I

Опция MIKEY-DHHMAC

В данном Дополнении описывается, как реализовать опцию управления ключами MIKEY-DHHMAC в данном профиле защиты.

Данная опция управления ключами подразумевает использование только инфраструктуры защиты, где доступны общие ключи. Благодаря возможностям, свойственным механизму Диффи-Хеллмана, MIKEY-DHHMAC (RFC 4650) обеспечивает качество защиты совершенной передовой секретности (PFS).таким образом, данная опция управления ключами применима, когда требуется PFS, а PKI или цифровые сертификаты не доступны.

Данный сценарий подразумевает наличие привратников внутри домена H.323.

Процедура, описанная в данном пункте, создает сквозной общий секрет между конечными точками H.323 EP A и EP B, используя схему согласования ключей Диффи-Хеллмана. Согласование ключей Диффи-Хеллмана происходит во время фазы регистрации и допуска RAS H.225.0, а, в случае многочисленных привратников, во время обмена сообщениями LRQ/LCF между привратниками. Сгенерированный общий секрет Диффи-Хеллмана служит в качестве сквозного ключа аутентификации и сохраняется в течение вызова. Протокол MIKEY-DHHMAC появляется во время установления вызова отдельно и создает секреты MIKEY на основе вызова для канала-носителя.

На рисунке I.1 изображен пример, где конечная точка B вызывает конечную точку A через маршрутизирующий GK. Сообщение проходит путь, аналогичный пути, изображенному на рисунке 4, за исключением того, что происходит развертывание протокола MIKEY-DHHMAC. Сценарий предполагает наличие одного или более маршрутизирующих привратников (модель, маршрутизируемая GK), где сообщения H.245 туннелируются в H.225.0 (Fast start). Сигнализация вызова может проходить или не проходить через привратник; поэтому не обязательно, чтобы маршрутизирующий привратник поддерживал данный сценарий.

ПРИМЕЧАНИЕ 1. – На схеме прохождения сообщения также изображен случай прямого соединения (без маршрутизирующего привратника), где обмен сообщениями сигнализации вызова между конечными точками происходит напрямую и не направляется привратниками.

На схеме, рисунок I.1, также показан базовый профиль защиты H.235.1, где каждое сообщение защищается полностью (аутентификация и целостность). Кроме того, сообщение проходит похожий путь при применении опции "только аутентификация" базового профиля защиты (на рисунке не показано). В таком случае HMAC вычисляется не по всему сообщению, а только по подмножеству (**ClearToken** в **CryptoToken**) сообщения RAS/H.225.0.

В примере прохождения сообщения показан случай, когда EP B (инициатор MIKEY) вызывает EP A (ответчик MIKEY), используя быстрый старт (см. рисунок I.1). Во время этапа 1 конечные точки H.323 A и B первоначально регистрируются на привратнике, используя **RRQ**, и предоставляют свои половины ключа DH (g^a и g^b). Для передачи половины ключа Диффи-Хеллмана во время **RRQ** и **ACF**. По этой причине не следует использовать поле **challenge**.

Половина ключа Диффи-Хеллмана должна передаваться в **dhkey** как часть **ClearToken**. ClearToken должно использовать OID "TG" (см. 8.5) вместо ClearToken OID "T" основного профиля H.235.1, показывающего, что данный профиль защиты используется вместе с H.235.1. Привратник должен сохранять каждую половину ключа пока конечная точка остается зарегистрированной. Если конечные точки выполняют подтверждение активности или используют упрощенную перерегистрацию (re-RRQ), они не должны включать половины ключа DH. **RCF** должно использовать OID "TG" в ClearToken для обозначения того, что привратник поддерживает данный профиль защиты.

EP B, пытающаяся вызвать EP A, запрашивает допуск у привратника D (**ARQ**). В сообщении **ARQ** в ClearToken должен использоваться OID "TG". OID "TG" должен также использоваться в ClearToken всех других сообщений RAS.

Сценарий охватывает многочисленных сцепленных привратников, но может равным образом поддерживать и одного привратника. Обнаружение удаленной конечной точки должно быть выполнено в соответствии с 8.1.6/H.323 "Дополнительная сигнализация вызываемой конечной точки" с использованием **LRQ/LCF**. Так инициирующая конечная точка определяет местонахождение зоны удаленного привратника и таким образом получает половину ключа DH вызываемой конечной точки. Если привратнику GK E необходимо определить местонахождение зоны удаленного привратника, привратник GK E должен послать сообщение **LRQ.** В случае многоадресной передачи generalID в CryptoToken сообщения **LRQ** не используется. Если привратник GK D не поддерживает данный профиль, он должен ответить сообщением **LRJ**. В противном случае привратник GK D должен ответить сообщением **LCF,** которое включает половину ключа DH конечной точки EP A. Затем привратник GK E должен ответить сообщением **ACF,** включающим половину ключа DH конечной точки EP A. Если привратнику GK E не удалось определить местонахождение удаленной конечной точки A, он отвечает сообщением **ARJ**.

Связь между двумя привратниками должна быть защищена в соответствии с H.235.1. Предполагается, что для этого доступен общий секрет *sl*. Поскольку сообщение **LRQ** среди привратников обычно является многоадресным, общий секрет *sl* обычно в действительности представляет собой не пару общих секретов, а группу общих секретов внутри потенциального скопления привратников. Данное предположение ограничивает масштабируемость в общем случае и не обеспечивает аутентификацию источника. Между тем, считается, что в корпоративных сетях с ограниченным небольшим числом проверенных привратников, подобные ограничения допустимы. Обеспечение защиты многоадресного взаимодействия между привратниками при помощи электронной подписи могло бы преодолеть данные ограничения; это, однако, остается предметом дальнейших исследований.

Конечная точка EP B получает половину ключа DH конечной точки EP A (**ACF**). Сообщение **ACF** должно содержать ключ DH вызываемой конечной точки в **dhkey** в основном **ClearToken** H.235.1, но используя идентификатор объекта OID "TG" вместо "T". Все остальные поля внутри **ClearToken** не должны подвергаться изменению данным профилем защиты.

ПРИМЕЧАНИЕ 2. – Конечные точки оперируют с половинами ключа DH, который остается статичным все время регистрации для всех вызовов. Это, однако, не является недостатком защиты, поскольку каждая конечная точка применяет половины ключа, выбранные случайным образом.

Тем не менее, конечные точки должны вводить новое случайное значение в 512 бит (т. е. 64 байта) в **challenge** наряду со своей половиной ключа DH, (см. RFC 2631, пункт 2.3). Данные значения **challenge** зависят от вызова и вносят необходимую произвольность и своевременность в генерирование ключа DH.

Затем исходящая конечная точка EP B может вычислить g^{ab} и динамический общий секрет $ZZ_{AB,}$ используя случайное значение в **challenge** и результат, полученный от MIKEY-PRF(g^{ab},0x12F905FE || **challenge**) (см. RFC 3830, пункты 4.1.2–4.1.4). Затем протокол MIKEY может вычислить ключ аутентификации (*Ma*), используя протокол MIKEY-PRF (см. RFC 3830, пункты 4.1.2–4.1.4).

Во время этапа 2 инициирующая EP B должна сгенерировать новые случайные значения MIKEY *y* и соответствующее g^y, а затем создать сообщение MIKEY I_message Imsg в соответствии с протоколом MIKEY-DHHMAC, использующим *Ma.*

Необходимо перевести сообщение MIKEY I_message в двоичный код.

Исходящей конечной точке EP B всегда следует включать свою половину ключа DH в **dhkey ClearToken**, таким образом делая возможной модель прямого соединения, поддерживаемую привратниками. Следует включить **ClearToken** в сообщение Setup и переслать его конечной точке EP A. Маршрутизирующий привратник должен направить передаваемое ClearToken на следующий переход (без внесения изменений в сообщение MIKEY).

Затем получающая конечная точка EP A вычисляет g^{ab} и динамический общий секрет ZZ_{AB} из MIKEY-PRF($g^{ab,}$, 0x12F905FE || **challenge**) (см. RFC 3830, пункты 4.1.2–4.1.4). Затем протокол MIKEY вычисляет код (*Me*) и ключи аутентификации (*Ma*), используя протокол MIKEY-PRF (см. RFC 3830, пункты 4.1.2–4.1.4). Затем EP A генерирует случайное значение MIKEY *w* и вычисляет g^{w}. Используя полученные половины ключа DH, EP A вычисляет *TGK.*

Затем из *TGK* получающая конечная точка EP A может вычислить ключи сессии SRTP, как описано в RFC 3711, пункт 4.3 (на рисунке не показано).

Конечная точка EP A создает аналогичное сообщение R_message Rmsg. Сообщение R_message передается внутри сообщения CallProceeding-to-Connect (CP/C). Rmsg представляет собой соответствующее сообщение ответа MIKEY, посылаемое EP B внутри сообщения CallProceeding-to-Connect (CP/C).

Сообщение CallProceeding-to-Connect (CP/C) посылается конечной точке EP B.

EP B извлекает половину ключа DH и вычисляет *TGK*. Затем EP B вычисляет ключи сессии SRTP из TGK, как описано в RFC 3711, пункт 4.3 (на рисунке не показано).

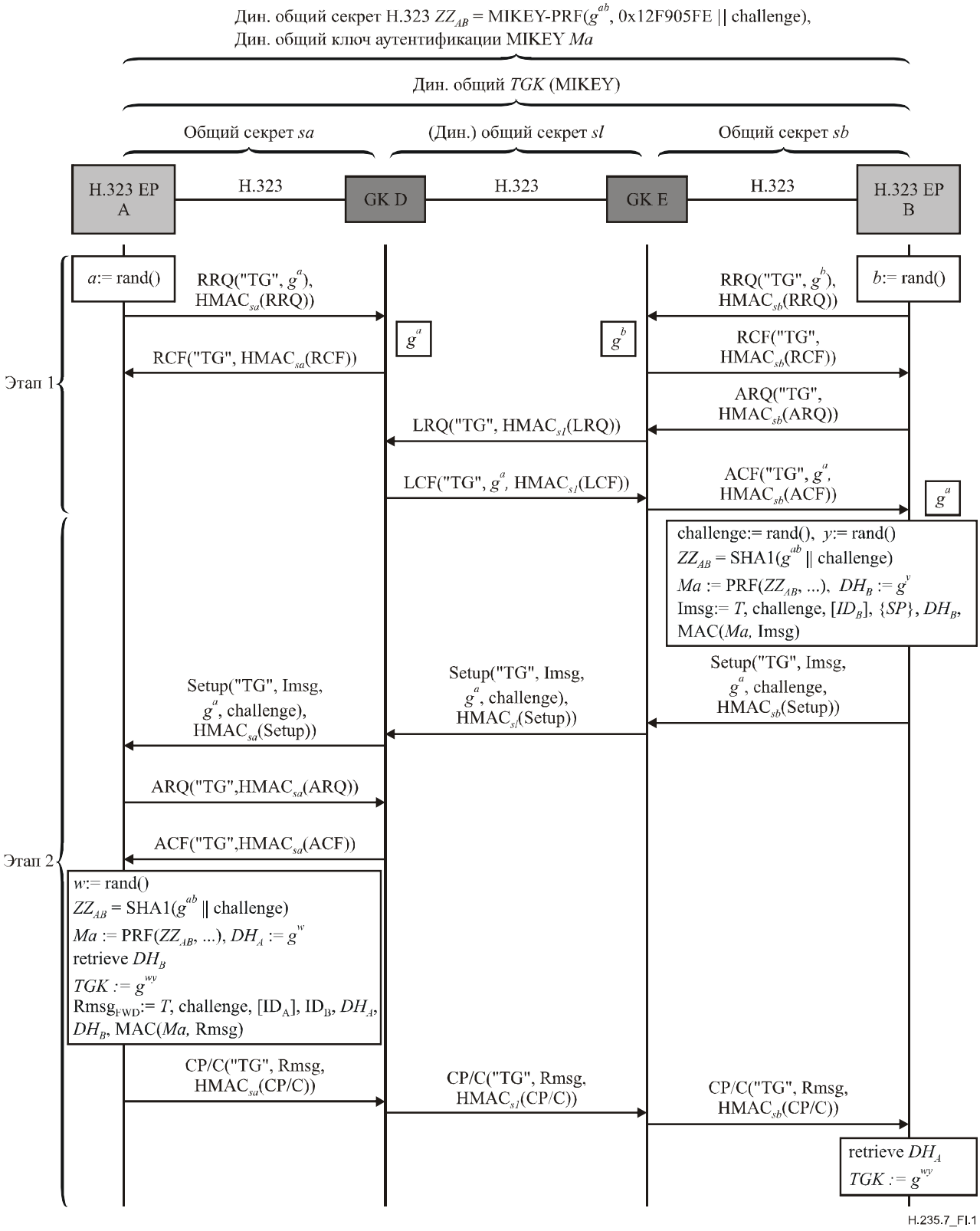

Рисунок I.1/H.235.7 – Пример: конечная точка B вызывает конечную точку A (маршрутизируемую привратником) с MIKEY-DHHMAC

I.1 Завершение вызова H.323

Поскольку вовлеченные конечные точки поддерживают состояние для MIKEY и SRTP, необходима подходящая процедура завершения. На рисунке I.2 изображен пример прохождения сообщений в случае, когда EP B (инициатор MIKEY) завершает вызов. В основном, поток проходит согласно 8.5/H.323 "Фаза E – Завершение вызова".

ПРИМЕЧАНИЕ. – На рисунке I.2 также показаны дополнительные процедуры разрыва соединения в случае, когда конечные точки полностью отменяют регистрацию. Затем конечные точки должны удалить частный ключ DH (*a* или *b*) и половину открытого ключа DH (g^a или g^b).

Поскольку процедура завершения вызова не зависит от данного профиля защиты, может быть использован любой применимый OID лежащего в основе профиля защиты (H.235.1, H.235.3, и т. д.); поэтому на рисунке I.2 OID не изображены.

Если конечная точка снова регистрируется на привратнике, должны быть сгенерированы новые половины ключа DH. Однако только для завершения вызова нет необходимости в полной отмене регистрации. Если конечная точка решает остаться зарегистрированной на привратнике, могут продолжать использоваться статические половины ключа DH.

В случае, когда конечные точки остаются зарегистрированными, и процедура разрыва соединения не применяется, конечные точки должны удалить только информацию, касающуюся вызова, включая соответствующую половину ключа DH, **challenge**, ключи MIKEY *Me*, *Ma*, *TGK* и информацию, касающуюся сессии SRTP.

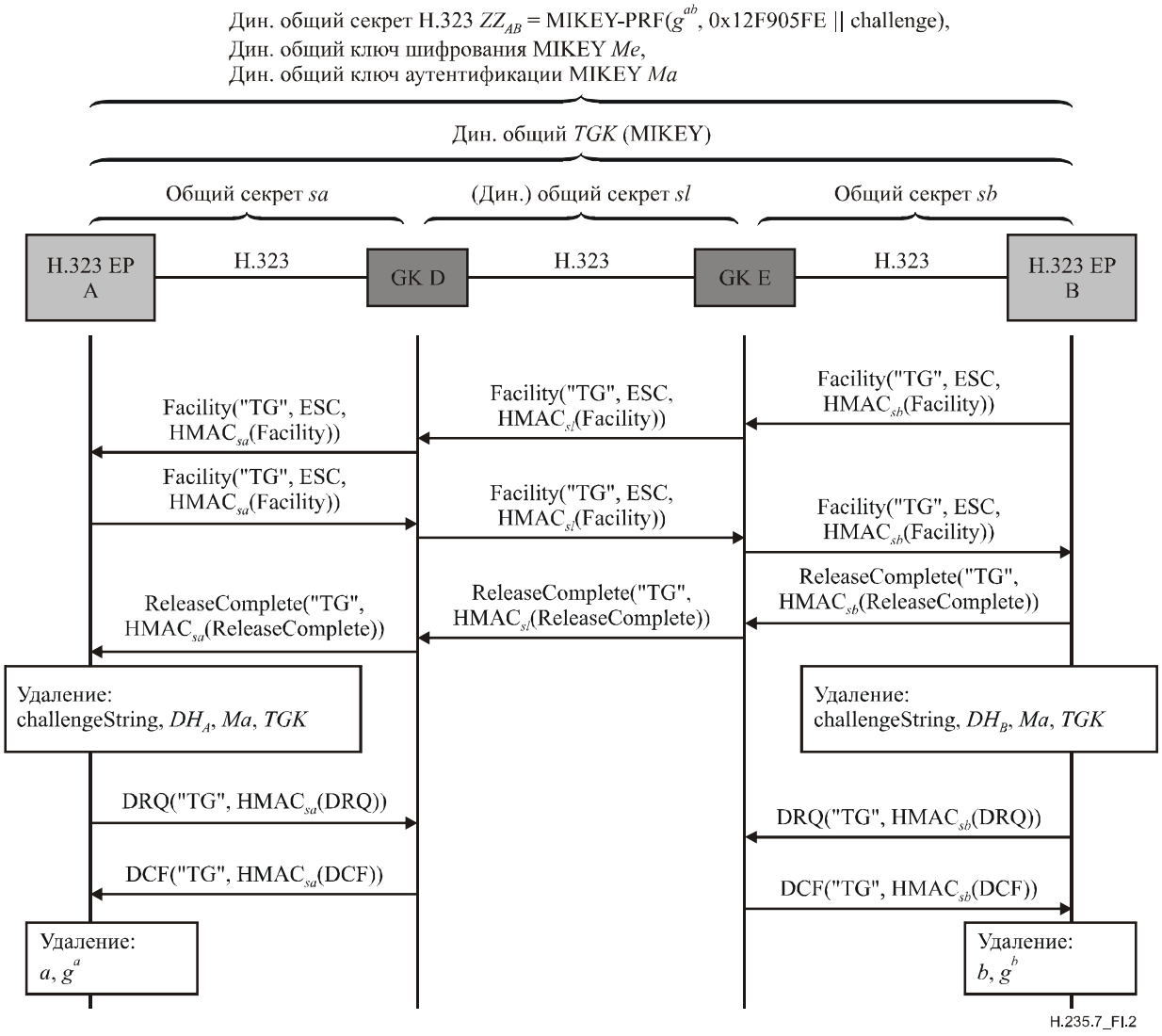

Рисунок I.2/H.235.7 – Пример: конечная точка B завершает вызов

I.2 Смена ключа шифрования TGK и обновление CSB

Протокол MIKEY имеет встроенную поддержку смены ключей шифрования TGK и/или обновления информации CSB. Профиль данной Рекомендации должен использовать для этой цели процедуру MIKEY-DHHMAC в RFC 4650, пункт 3.1, которая позволяет обновить TGK до окончания срока действия, или обновить другую информацию(CSB), не внося изменений в TGK.

Механизм смены ключей шифрования TGK и обновления CSB полезен для обеспечения защиты пакета логических каналов в рамках одной политики защиты. Для этого рекомендуется выполнять/запускать (полный) протокол MIKEY-DHHMAC, как описано выше, только для первого логического канала. Все последующие логические каналы, которые должны применять одну и ту же политику защиты MIKEY или один и тот же TGK, должны использовать механизм обновления CSB без механизма смены ключей шифрования в данном пункте, делая ссылку на первоначальный идентификатор CSB-ID и пропуская обновленные данные TGK. Это позволяет настроить логические каналы или крипто сессии MIKEY эффективнее, чем при запуске полного протокола MIKEY на каждом логическом канале.

Сообщения смены ключа шифрования TGK MIKEY или обновления CSB должны включаться и передаваться в **MiscellaneousCommand** внутри сообщения Facility message. Значение **tokenOID ClearToken** должно быть выставлено на "TG".

Для протокола MIKEY на "уровне медиа" конечная точка EP B определяет, на каком логическом канале будет применяться смена ключей шифрования TGK и/или обновление CSB. Конечная точка EP A, будучи ответчиком, также будет использовать **MiscellaneousCommand** в сообщении Facility для передачи MIKEY R_message (при наличии).

Для смены ключей шифрования TGK (см. рисунок I.3), EP B, будучи инициатором MIKEY, должна сгенерировать новый TGK. **parameterValue** должно содержать соответствующее сообщение MIKEY I_message в двоичном коде.

EP A, будучи ответчиком, может подтвердить полученное сообщение о смене шифровальных ключей TGK, если этого требует конечная точка EP B. EP A создает аналогичное сообщение R_messages. Сообщение R_message передается внутри сообщения Facility. EP B посылает сообщение Facility на EP A.

Для обновления CSB инициированного инициатором, процедура аналогична за исключением того, что сообщение MIKEY не должно содержать TGK.

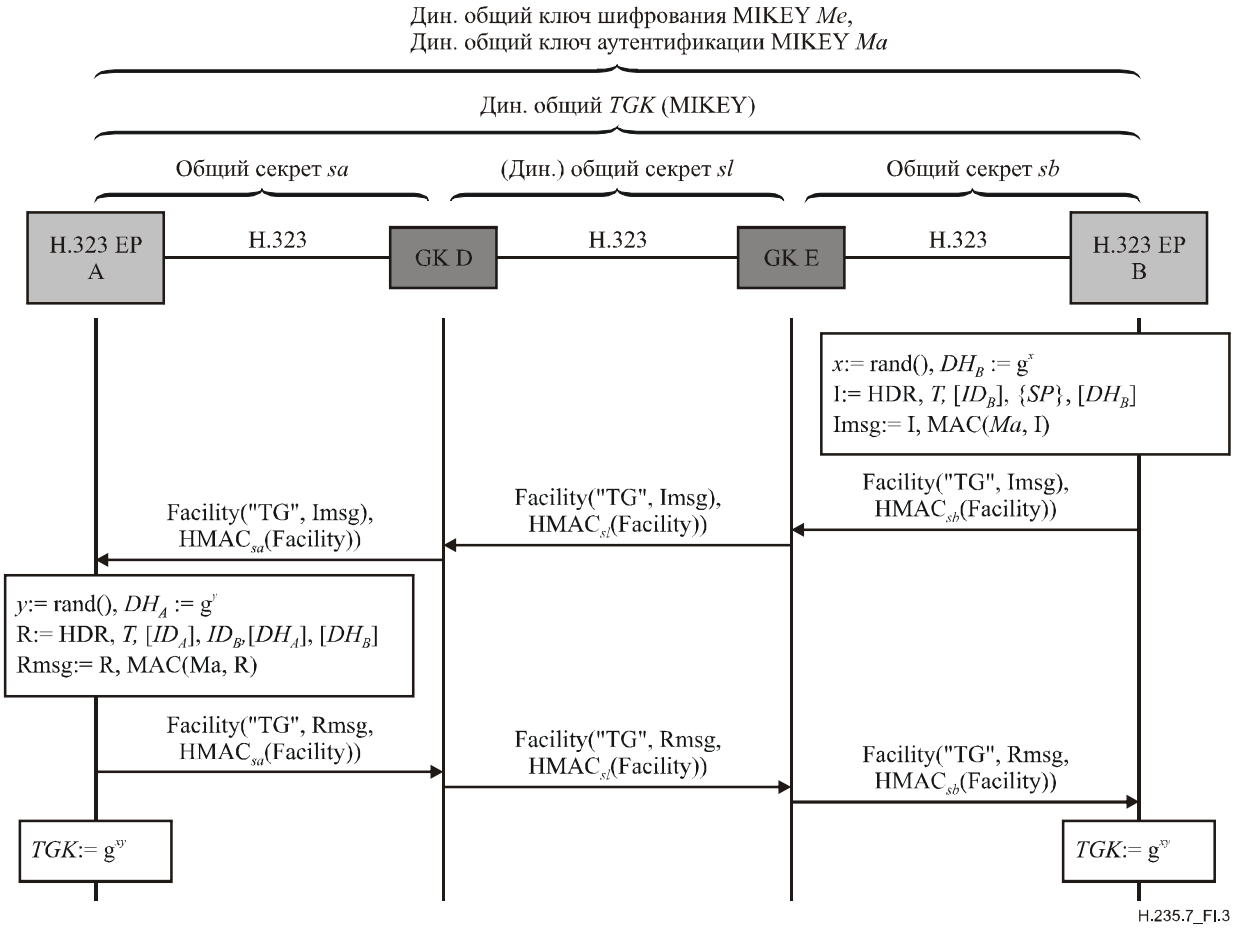

Рисунок I.3/H.235.7 – Пример: конечная точка B обновляет ключ

В данной Рекомендации не определяются процедуры для смены ключей шифрования TGK и/или обновления CSB, инициируемых ответчиком; это является предметом дальнейшего исследования.

Дополнение II

Использование H.235.4 для создания предварительного общего секрета

В данном Дополнении описывается, как реализовать процедуру DRC1 Рекомендации МСЭ-Т H.235.4 для создания предварительного общего секрета ZZAB между конечными точками B и A, предположив, что априори такого сквозного секрета не существует. Метод, описанный в данном Дополнении, применим к сценариям с одним или многочисленными привратниками. Процедура, описанная в Дополнении, не включает вычисление DH во время регистрации или допуска RAS, а использует симметричную криптографию.

На рисунке II.1 изображен пример схемы прохождения сообщения в случае, когда конечная точка B вызывает конечную точку A.

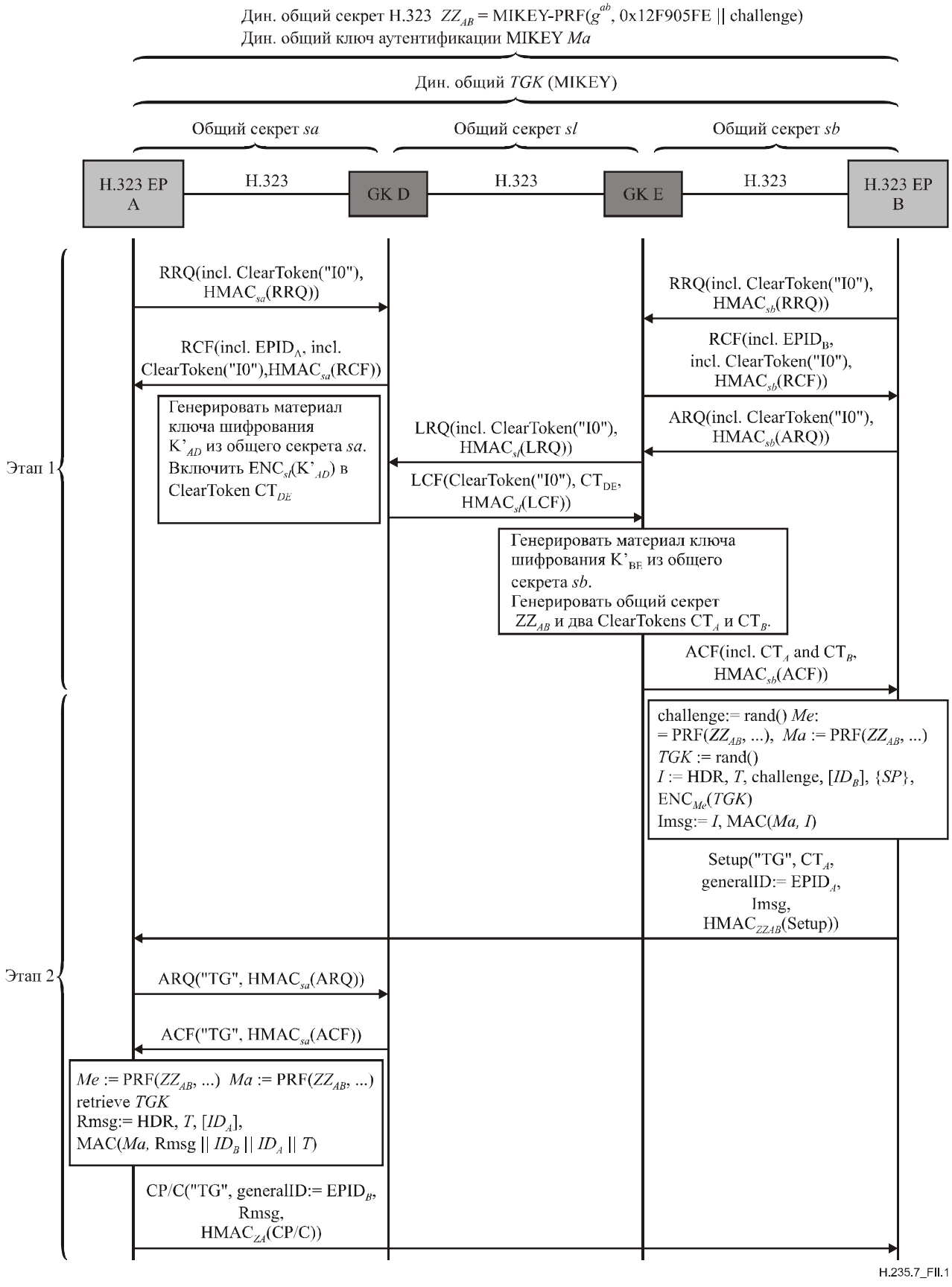

Рисунок II.1/H.235.7 – Пример: конечная точка B вызывает конечную точку A (не маршрутизируемую привратником) с предварительным общим секретом MIKEY и DRC1 H.235.4

II.1 Завершение вызова H.323

Завершение вызова H.323 должно происходить, как описано в пункте 8.1.

II.2 Смена ключей шифрования TGK и обновление CSB

Смена ключей шифрования TGK и/или обновление CSB должно происходить, как описано в пункте 8.2.

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 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.