МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

H.235.3

(09/2005)

СЕРИЯ H: АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

Инфраструктура аудиовизуальных услуг – Системные аспекты

Безопасность H.323: Гибридный профиль защиты

Рекомендация МСЭ-Т H.235.3

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.235.3

Безопасность H.323: Гибридный профиль защиты

Резюме

Целью данной Рекомендации является описание эффективности и масштабируемости гибридного профиля защиты, основанного на PKI (инфраструктура управления открытыми ключами) для версии 2 или выше последующих Рекомендаций МСЭ-Т H.235.0. Гибридный профиль защиты включает в себя преимущества защитных профилей из Рекомендаций МСЭ-Т H.235.1 и H.235.2, а именно: цифровую подпись из Рекомендации МСЭ-Т H.235.2 и базовый профиль защиты из Рекомендации МСЭ-Т H.235.1.

В предыдущих версиях Рекомендаций МСЭ-Т подсерии H.235 данный профиль содержался в Приложении F/H.235. В Дополнениях IV, V, VI к Рекомендации МСЭ-Т H.235.0 приводятся полные соответствия между пунктами, рисунками и таблицами версий 3 и 4 Рекомендации МСЭ-Т H.235.

Источник

Рекомендация МСЭ-Т H.235.3 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, сертификат, цифровая подпись, шифрование, целостность, управление ключами, защита мультимедиа, профиль защиты.

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

Рекомендации МСЭ-Т H.235.3

Безопасность H.323: Гибридный профиль защиты

1 Сфера применения

Целью данной Рекомендации является описание эффективности и масштабируемости гибридного профиля защиты, основанного на PKI (инфраструктура управления открытыми ключами) для версии 2 или выше последующих Рекомендаций МСЭ-Т H.235.0. Гибридный профиль защиты включает в себя преимущества защитных профилей из Рекомендаций МСЭ-Т H.235.1 и H.235.2, а именно: цифровую подпись из Рекомендации МСЭ-Т H.235.2 и базовый профиль защиты из Рекомендации МСЭ-Т H.235.1.

2 Справочные документы

2.1 Нормативные справочные документы

В перечисленных ниже Рекомендациях МСЭ-Т и других справочных документах содержатся положения, которые посредством ссылок на них в этом тексте составляют основные положения данной Рекомендации. На момент опубликования, действовали указанные редакции документов. Все Рекомендации и другие справочные документы являются предметом корректировки, 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 г.), *Протоколы сигнализации о соединении и пакетирование потоков носителей для мультимедийных систем связи на основе пакетов*.

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

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

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

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

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

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

– ITU-T Recommendation H.245 (2005 г.), *Управляющий протокол для мультимедийной связи*.

– ITU-T Recommendation H.323 (2003 г.), *Мультимедийные системы связи на основе пакетов*.

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

– ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

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

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

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

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

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

– IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

2.2 Информативные справочные документы

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

[PKCS] PKCS #1 v2.0: *RSA Cryptography Standard;* RSA Laboratories; October 1, 1998; http://www.rsa.com/rsalabs/pubs/PKCS/index.html.

[PKCS] PKCS #7: *Cryptographic Message Syntax Standard*, An RSA Laboratories Technical Note, version 1.5, Revised November 1, 1993; http://www.rsa.com/rsalabs/pubs/PKCS/index.html.

[RFC1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm*.

3 Термины и определения

Наряду с определениями, данными в этом пункте, также используются определения, данные в пунктах 3/H.323, 3/H.225.0 и 3/H.245. Некоторые из оконечных устройств, используемых в данной Рекомендации, также определяются в Рекомендациях МСЭ-Т: X.800| ИСО 7498-2, X.803 | ИСО/МЭК 10745, X.810 | ИСО/МЭК 10181-1, X.811 | ИСО/МЭК 10181-2, H.235.0.

4 Сокращения

В Рекомендации используются следующие сокращения:

ALG	Application Level Gateway	Шлюз уровня приложения
ASN.1	Abstract Syntax Notation One	Абстрактно-синтаксическая нотация версии 1
BRJ	Bandwidth Reject	Отклонение полосы пропускания
BRQ	Bandwidth Request	Запрос полосы пропускания
CA	Certification Authority	Орган сертификации
CRL	Certificate Revocation List	Список аннулированных сертификатов
DB	Database	База данных
DH	Diffie-Hellman	Алгоритм Диффи-Хеллмана
DN	Distinguished Name	Отличительное имя
EP	Endpoint	Конечная точка
GCF	Gatekeeper Confirm	Подтверждение привратника
GK	Gatekeeper	Привратник
GKID	Gatekeeper Identifier	Идентификатор привратника
GKSP	Gatekeeper Security Processor	Процессор защиты привратника
GRJ	Gatekeeper Reject	Отклонение привратника
GRQ	Gatekeeper Request	Запрос привратника

HMAC	Hashed Message Authentication Code	Код аутентификации сообщения, использующий хэш-функцию
ICV	Integrity Check Value	Значение проверки целостности
ID	Identifier	Идентификатор
IP	Internet Protocol	Протокол Интернет
LDAP	Lightweight Directory Access Protocol	Облегченный протокол доступа к справочнику
LRQ	Location Request	Запрос местонахождения
MCU	Multipoint Control Unit	Блок управления многоточечной связью
MD5	Message Digest 5	Односторонняя хэш-функция MD5
NAT	Network Address Translation	Трансляция сетевых адресов
OID	Object Identifier	Идентификатор объекта
PDU	Protocol Data Unit	Протокольный блок данных
PKI	Public Key Infrastructure	Инфраструктура управления открытыми ключами
RAS	Registration, Admission and Status	Регистрация, допуск и статус
RCF	Registration Confirm	Подтверждение регистрации
RRJ	Registration Reject	Отклонение регистрации
RRQ	Registration Request	Запрос регистрации
RSA	Rivest, Shamir and Adleman encryption algorithm	Алгоритм шифрования Райвеста, Шамира и Адлемана
RTP	Real-time Transport Protocol	Транспортный протокол режима реального времени
SHA	Secure Hash Algorithm	Надежный алгоритм хеширования
UDP	User Datagram Protocol	Протокол дейтаграмм пользователя
URQ	Unregistration Request	Запрос о снятии регистрации
VoIP	Voice-over-IP	Передача голоса через протокол Интернет

5 Соглашения по терминам

В этой Рекомендации используются следующие соглашения:

– "должен" означает обязательное требование;

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

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

Для определения понятия гибридного профиля защиты используются термины и определения, содержащиеся в Рекомендациях МСЭ-Т H.235.1 и H.235.2.

Служба целостности сообщения всегда обеспечивает аутентификацию сообщения, но не наоборот. В режиме "только аутентификация" гарантированная целостность охватывает только определенное подмножество полей сообщения. Данное утверждение справедливо и для служб целостности, реализуемых ассиметричными средствами (например, цифровые подписи). Таким образом, на практике, комбинированная служба аутентификации и целостности использует один и тот же материал ключа с сохранением защиты.

Данный профиль защиты применяется в сетевом окружении с потенциально большим числом оконечных устройств, где статическое присвоение пароля/симметричного ключа неприемлемо, например, в сценариях большого или глобального масштаба. Кроме того, данный профиль защиты предполагает доступность инфраструктуры открытого ключа с выделенными сертификатами и

частными/открытыми ключами, справочников и т. д. В дополнении к этому в данном профиле защиты используется симметричная техника шифрования.

В данном профиле защиты используются термины "первое" посылаемое сообщение и "последнее" посылаемое сообщение. Обеспечение защиты для первого сообщения (и возможно также для последнего сообщения) отличается от обеспечения защиты для других сообщений, посылаемых между указанными выше.

Посылаемое "первое сообщение" представляет собой сообщение, которое протекает между двумя объектами H.323 и устанавливает среду защиты. Это позволяет сделать симметричный материал ключа доступным для обоих объектов и, к примеру, помечать начало вызова. Для RAS H.225.0, первое сообщение – это запрос регистрации (RRQ Registration Request) и сопутствующее отосланное сообщение. Для сигнализации вызова H.225.0 используют быстрый старт, первое сообщение это "SETUP and CONNECT".

"Последнее сообщение" завершает установленную среду защиты. Установленный материал ключа должен быть уничтожен. Для стандартов RAS H.225.0, последнее сообщение – это запрос о снятии регистрации URQ и сопутствующее отосланное сообщение, для сигнализации вызова H.225.0 последним сообщением является "RELEASE-COMPLETE".

6 Общие положения

В данной рекомендации описывается эффективность и масштабируемость гибридного профиля защиты, основанного на PKI, в котором используется цифровая подпись из Рекомендации МСЭ-Т H.235.2 и базовый профиль защиты из Рекомендации МСЭ-Т H.235.1. Данная Рекомендация предлагается в качестве дополнения. Объекты защиты H.323 (оконечные устройства, привратники, шлюзы, узлы контроля многоточечной связи (MCU) и т. д.) могут приводить в исполнение данный гибридный профиль защиты для усовершенствования защиты или по требованию.

Понятие "гибридный" в этом тексте должно означать, что процедуры защиты для профиля защиты цифровой подписи из Рекомендации МСЭ-Т H.235.2 в действительности применяются лишь в некоторых случаях, и цифровые подписи все же больше соответствуют процедурам RSA. Тем не менее, цифровые подписи используются только при крайней необходимости, в случае, когда очень эффективные симметричные методы защиты из базового профиля защиты Рекомендации МСЭ-Т H.235.1 использованы полностью.

Гибридный профиль защиты применим в масштабируемой "глобальной" IP-телефонии. Данный профиль защиты преодолевает ограничения базового профиля защиты H.235.1. Более того, данный профиль защиты преодолевает существующие недостатки стандарта H.235.2, такие как необходимость в большей полосе пропускания и увеличении производительности, необходимой для обработки данных. Например, гибридный профиль защиты не зависит от (статического) администрирования общих секретов переходов в различных доменах. Таким образом, пользователи могут просто воспользоваться их поставщиком услуг передачи голоса через протокол Интернет (VoIP). Данный профиль защиты также поддерживает существующие разновидности мобильности пользователей. В профиле применяется ассиметричное шифрование с цифровыми подписями и сертификатами только по необходимости, а во всех остальных случаях, используется более простые и эффективные симметричные методы. Это обеспечивает туннелирование сообщений H.245 для сохранения целостности сообщений H.245 а также обеспечивает выполнение некоторых условий для неотказуемости сообщений.

Гибридный профиль защиты подразумевает использование модели GK-маршрутизации, и основывается на методах туннелирования H.245. Поддержка моделей, основанных не на GK-маршрутизации, является материалом для дальнейшего изучения.

Возможности, предоставляемые данными профилями, включают:

Для сообщений RAS H.225.0 и H.245:

– Аутентификация пользователя и необходимая целостность независимо от количества переходов прикладного уровня, которые проходит сообщение.

  ПРИМЕЧАНИЕ 1. – "Переход" в данном случае понимается как доверенный элемент сети H.235 (например, привратник, шлюз, узел MCU, прокси, брандмауэр). Таким образом, последовательная (по звеньям переходов – hop-by-hop) защиты уровня приложения при использовании симметричных методов не обеспечивает истинную сквозную защиту между оконечными устройствами.

– Целостность всех необходимых частей (полей) сообщений, приходящих на объект независимо от количества переходов уровня приложения, которые проходят сообщения. Также дополнительной является возможность обеспечения целостности самого сообщения с использованием порожденного случайного числа.

– Аутентификация, целостность и (некоторый) неотказуемость переходного сообщения уровня приложения предоставляют эти услуги защиты всему сообщению.

– Использование доступной инфраструктуры открытого ключа, пользователи могут выбирать своего служебного провайдера. Управление ключами для распределения сеансового ключа интегрировано в гибридный профиль защиты.

Используя вышеперечисленные службы защиты соответствующим образом, можно предотвратить некоторые виды атак, среди них:

– *Атаки через посредника*: от подобных атак защищает последовательная аутентификация и проверка целостности сообщения уровня приложений, если посредник, скажем, враждебный маршрутизатор, находится между переходами уровня приложения.

– *Атаки замещением оригинала*: такие атаки предотвращаются с помощью использования отметок времени и порядковых номеров

– *Имитация соединения (спуфинг)*: такие атаки отражает использование аутентификации пользователя.

– *Захват соединения*: такие атаки предотвращает аутентификация/целостность для каждого сообщения сигнализации.

В данном профиле защиты используется модель вызова GK-маршрутизации, в которой применяется метод сигнализации вызова быстрого соединения. Контроль вызова сообщений H.245.0 надежно туннелируется в сообщениях сигнализации вызова H.225.0 и наследует, таким образом, схему обеспечения защиты H.225.0.

Профиль защиты цифровой подписи позволяет надежно туннелировать модули данных протоколов (PDU) контроля вызова H. 245 внутри аппаратных сообщений H.225.0. Обновление ключей H.245 и механизмы синхронизации требуют туннелирования для сообщений FACILITY обновления ключей, которые должны быть сигнализированы,_туннелирование также является полезным, например, при очень продолжительных вызовах.

Участок с диагональной штриховкой в таблице 1 показывает механизмы защиты, которые используются в гибридном профиле защиты.

ПРИМЕЧАНИЕ 2. – Сертификаты RSA с MD5 ([RFC1321]) хэшируются и не являются частью данного профиля защиты.

Вместе с гибридным профилем защиты можно дополнительно использовать профиль защиты шифрования голоса H.235.6 (см. 6.1/H.235.6). Данное использование реализуется как часть сигнализации установки вызова.

Таблица 1/H.235.3 – Общие положения гибридного профиля защиты

Службы защиты	Функции вызова			
	RAS	**H.225.0**	**H.245 (Примечание 3)**	**RTP**
Аутентификация	цифровая подпись RSA (SHA1)	цифровая подпись RSA (SHA1)	цифровая подпись RSA (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
Неотказуемость	(возможно только в первом сообщении)	(возможно только в первом сообщении)		
Целостность	цифровая подпись RSA (SHA1)	цифровая подпись RSA (SHA1)	цифровая подпись RSA (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
Конфиденциальность				
Контроль доступа				
Управление ключами	распределение сертификата	распределение сертификата		
	аутентифицированный обмен ключами Диффи-Хеллмана	аутентифицированный обмен ключами Диффи-Хеллмана		

ПРИМЕЧАНИЕ 1. – Необходимо, чтобы гибридный профиль защиты поддерживался другими объектами H.235 (например, привратниками, шлюзами и модулями доступа H.235)

ПРИМЕЧАНИЕ 2. – Доступные биты использования ключей в сертификате также могут определять службу защиты, предоставляемую оконечным устройством (например, утвержденная неотказуемость).

ПРИМЕЧАНИЕ 3. – Сообщение H.245, туннелированное или инкапсулированное в сообщение H.225.0 быстрого соединения.

Данная Рекомендация может использовать защиту целостности сообщения, которая охватывает все сообщение целиком. Для RAS H.225.0 защита целостности охватывает все сообщение RAS; для сигнализации вызова защита целостности охватывает все сообщение сигнализации вызова H.225.0, включая заголовки Q.931.

Для аутентификации пользователю следует использовать схему цифровой подписи открытого/частного ключа. Такая схема обычно обеспечивает лучшую целостность и неотказуемость вызова.

В данной Рекомендации не описываются процедуры для: регистрации, сертификации, и предоставления сертификатов от доверенного центра и назначения частного/открытого ключа, службы каталогов, специальных (особых) параметров CA, аннулирования сертификата, обновления/восстановления криптографической пары и других процедур по работе и управлению сертификатами таких, как сертификат или частный/открытый ключ и доставка и инсталляция сертификатов в оконечные устройства. Такие процедуры могут осуществляться средствами, которые не являются частью данной Рекомендации.

Объекты связи, участвующие в процессе, могут, в неявном виде, определять использование базовых профилей защиты H.235.1, профиля защиты цифровой подписи H.235.2 или данного гибридного профиля защиты, оценивая сигнализированные идентификаторы объектов защиты в сообщениях (**tokenOID** и **algorithmOID**; см. также пункт 10/H.235.2).

6.1 Требования H.323

Предполагается, что объекты H. 323, которые применяют данный гибридный профиль защиты, поддерживают следующие характеристики H.323:

– быстрое соединение;

– туннелирование H.245; и

– модель GK-маршрутизации.

6.2 Аутентификация и целостность

В данной Рекомендации по предоставлению услуг защиты используются следующие термины:

Аутентификация и целостность: Это комбинированная служба защиты, которая поддерживает целостность сообщения при аутентификации пользователя. Аутентификация пользователя происходит, если либо пользователь поставил верную цифровую подпись под определенными данными с помощью частного ключа, либо при правильном применении связанного, общего секрета. Кроме того, сообщение защищено от несанкционированного использования. Обе службы защиты обеспечиваются одним и тем же алгоритмом защиты. Совмещение аутентификации и целостности возможно только на последовательном (переход-к-переходу, hop-to-hop) принципе.

ПРИМЕЧАНИЕ. – При использовании цифровых подписей может поддерживаться служба неотказуемости. Это также зависит от настроек битов использования ключа для подписанного ключа в сертификате (см. также RFC 3280).

Следующие процедуры описаны для использования данного профиля.

Процедура IV основывается на цифровых подписях, использующих криптографическую пару частного/открытого ключей для обеспечения аутентификации, целостности и неотказуемости сообщений RAS, Q.931 и H.245. Оконечные устройства могут использовать данный метод, если требуется эффективность и масштабируемая защита.

В зависимости от политики защиты аутентификация может быть односторонней или взаимной (т. е. применяющая аутентификацию/целостность в обратном направлении и, таким образом, обеспечивающая более высокий уровень защиты). Для режима защиты предпочтительнее использовать взаимную аутентификацию.

Привратники, обнаружившие отказ в аутентификации и/или неудовлетворительную проверку целостности данных в сообщении RAS /сообщении сигнализации вызова, полученном от оконечного устройства /другого привратника, отвечают соответствующим сообщением отказа, показывающим повреждение защиты, выводя **securityDenial** или другой подходящий код ошибки защиты в качестве причины отказа, согласно 11.1/H.235.0. В зависимости от способности распознать атаку и наиболее подходящего способа реагирования на нее, привратнику, получившему защищенное сообщение **xRQ** с неопределенными идентификаторами объекта (**tokenOID**, **algorithmOID**), следует ответить незащищенным сообщением **xRJ**, выводя в качестве причины отказа **securityDenied**, или удалить это сообщение. Конечная точка должна удалить полученное незащищенное сообщение, сделать паузу и может попытаться снова, выбрав другие идентификаторы объектов. Так же привратнику, получившему защищенное сообщение сигнализации SETUP H.225.0 с неопределенными идентификаторами объекта (**tokenOID**, **algorithmOID**), следует ответить незащищенным сообщением RELEASE COMPLETE, выводя в качестве причины отказа **securityDenied**, или отклонить это сообщение, в то время как, привратнику, получившему защищенное сообщение FACILITY H.225.0 с неопределенными идентификаторами объекта (**tokenOID**, **algorithmOID**), следует ответить незащищенным сообщением FACILITY, выводя в качестве причины **undefinedReason**, или отклонить это сообщение. Данное событие также следует занести в журнал регистрации. В части ответного сообщения, отправитель может высылать список допустимых сертификатов в отдельных полях, для того чтобы получателю было легче выбирать подходящий сертификат.

Существует неявная сигнализация H.235 для указания использования процедуры IV и применяемого алгоритма защиты, основывающаяся на значении идентификаторов объекта (см. также пункт 13) и заполненных полей сообщения. В данной рекомендации идентификаторы объекта символически обозначаются буквами (например, "A").

Данный профиль не использует поля значения проверки целостности (ICV) H.235. Скорее, криптографические значения проверки целостности вносятся в поле **signature** маркера **token** в **cryptoSignedToken**, когда речь идет о H.235.2, или значения проверки целостности вносятся в поля хэша в **CryptoToken**, когда имеется ввиду H.235.1.

7 Процедура IV

Если для обеспечения последовательной защиты используется процедура IV, необходимо соблюдать следующие процедуры. Данная процедура объединяет процедуру I пункта 7/H.235.1 и процедуру II пункта 7/H.235.2.

Для первого сообщения, включающего соответствующие ответы, посылаемые в каждом направлении, процедура II (последовательная аутентификация и целостность, см. пункт 7/H.235.2) должна быть использована со следующими установками:

– Идентификатор объекта (OID) "A1" вместо идентификатора объекта (OID) "A" и идентификатор объекта "S1" вместо идентификатора объекта "S". Использование этих идентификаторов объекта позволяет идентифицировать гибридный профиль защиты.
– **algorithmOID** в **tokenOID** должен быть со значением "W", указывающим на использование подписи RSA-SHA1.
– **signature** должна содержать подпись ASN.1 (Абстрактно-синтаксическая нотация версии 1), зашифрованную RSA (см. пункт 12/H.235.2).
– **certificate** должен бы содержать пользовательский сертификат отправителя, если иным путем он недоступен получателю; **type** должен содержать идентификатор объекта "W" указывающий сертификат, содержащий в себе RSA-SHA1 или идентификатор объекта "P" (см. пункт 20/H.235.2) указывающий, что **certificate** содержит URL.

В сценарии домена с одним администратором, "первое сообщение /ответ" определяется равным начальному значению сообщения /ответ RAS H.225.0; это обычно либо GRQ/GCF или RRQ/RCF. В сценарии домена с многими администраторами, первое сообщение /ответ внутри каждого домена определяется как указано выше; первое сообщение между доменами определяется как SETUP.

Всякий раз, когда цифровой сертификат передает сообщение, получающий объект должен сверять идентичность отправителя с идентичностью сертификата, согласно процедуре, описанной в пункте 14/H.235.2, с целью предотвращения атаки через посредника.

Отправитель и получатель обмениваются и вычисляют битовую строку, определяемую с помощью аутентифицированного секрета Диффи-Хеллмана. В таблице 4/H.235.6 приводятся примеры групповых параметров Диффи-Хеллмана и, в целях защиты, рекомендуется применять 1024-битовое простое число везде, где это возможно. Секрет Диффи-Хеллмана должен вычисляться для каждой ветви, независимо от того, используется профиль шифрования голоса или нет.

Из общей битовой строки, которую вычисляют обе стороны, обе стороны получают 160-битовый секрет, беря наименее значимые 160 бит. Полученный 160-битовый секрет записывается как пароль с общим секретом, который используется в Рекомендации МСЭ-Т H.235.1.

В сценарии с использованием привратника в отдельных административных доменах, получатель и отправитель должны использовать два поля в каждом направлении для сигнализации вызова H.225.0:

– Маркер **ClearToken** внутри **CryptoToken**, которое используется для вычисления медиа ключа, используемого совместно между оконечными устройствами (см. 8.5/H.235.6). Это необходимо только в случае, если используется шифрование голоса.
– **ClearToken** используется для вычисления ключа связи, который используется совместно получающим и отправляющим объектами, в целях защиты связи сигнализации. Данный ключ связи перемещает общий пароль среди привратников в H.235.1. Маркер **tokenOID** в **ClearToken** должен иметь значение "Q", это означает использование алгоритма Диффи-Хеллмана и гибридного профиля защиты. Вычисление ключа связи происходит по той же схеме, что и вычисление медиаключа. (см. 8.5/H.235.6).

ПРИМЕЧАНИЕ 1. – Для средств прямой маршрутизации, объектов отправителя/получателя и оконечного оборудования, соответственно. Для средств GK-маршрутизации, ключ связи разделяется последовательно (по звеньям переходов – hop-by-hop) между каждой парой равных привратников, тогда как медиаключ общий по сквозному принципу.

Для средств GK-маршрутизации, привратник должен направлять полученный маркер Диффи-Хеллмана от конечной точки к следующему переходу.

Для всех сообщений, но в первую очередь, для сообщения/ответа, посылаемых в каждом направлении, должна быть использована процедура I H.235.1 (см. пункт 7/H.235.1). Даная процедура также применяется в сценарии, когда многочисленные привратники располагаются внутри административного домена. В данном случае нет необходимости в использовании асимметричного управления ключами; вместо этого достаточно использовать H.235.1.

Данная Рекомендация может быть использована в системах H.235 версии 1, когда речь идет об ограниченном использовании sendersID и generalID, указанное применение описано в пункте 19/H.235.2.

Предполагается, что привратник может получать от индивидуальной фиксированной конечной точки только одно **RRQ**, включающий в себя маркер DH с цифровой подписью. Тем не менее, при использовании другого подписанного **RRQ**, потерянные или задержанные сообщения **RCF**/**RRJ** могут быть оправлены на ретрансляцию.

В случае преждевременного прибытия соответствующего ответа регистрации на конечную точку конечная точка может предпринять еще одну попытку. Для этого конечной точке следует использовать самый последний маркер Диффи-Хеллмана, но необходимо воспользоваться новым порядковым номером и новой отметкой времени.

Для определенно фиксированной конечной точки, привратник должен использовать самое последнее полученное подписанное сообщение **RRQ** и извлечь общий секрет из этого поля Диффи-Хеллмана, вне зависимости от того, имеется уже у привратника доступный общий секрет или нет. Таким образом, привратник должен переписать любой уже существующий общий секрет на новый, извлеченный им секрет. Привратник должен ответить с помощью подписанного **RCF**, что у него есть ответный маркер Диффи-Хеллмана. Предпочтительнее, чтобы ответный маркер Диффи-Хеллмана было сгенерирован заново.

ПРИМЕЧАНИЕ 2. – Выбранный и рекомендованный способ для обновления ключа осуществляется путем использования сообщения FACILITY, данный способ описывается в пункте 9. Тем не менее, оказывается, что обновление ключа может быть достигнуто путем использования дополнительного подписанного RRQ с новым маркером Диффи-Хеллмана.

ПРИМЕЧАНИЕ 3. – Привратник, обладая общим секретом, может отослать защищенное HMAC ответное сообщение защищенному HMAC сообщению RRQ (согласно Рекомендации МСЭ-Т H.235.1).

8 Защищенное соединение для одновременных вызовов

Оптимизация предоставляется для случая, когда фиксированная пара объектов может обрабатывать несколько независимых параллельных вызовов, используя при этом один канал сигнализации вызова. Вместо установленных нескольких ключей связи с алгоритмом Диффи-Хэллмана для каждого вызова защищенное соединение определяет, какой из многочисленных одновременных вызовов охватить.

Точнее, защищенное соединение охватывает все вызовы между фиксированной парой объектов до тех пор, пока работает канал сигнализации вызова. Объекты используют флаг **multipleCalls** в процедуре Setup, для того чтобы показать возможность сигнализации множественных вызовов через соединение сигнализации одиночного вызова (см. 7.3/H.323).

Если используется одно соединение сигнализации вызова, то требуется установить только один общий ключ связи, см. рисунок 1.

С другой стороны, если в процедуре SETUP не установлен флаг **multipleCalls**, то ключ связи должен быть вычислен заново для каждого вызова индивидуально.

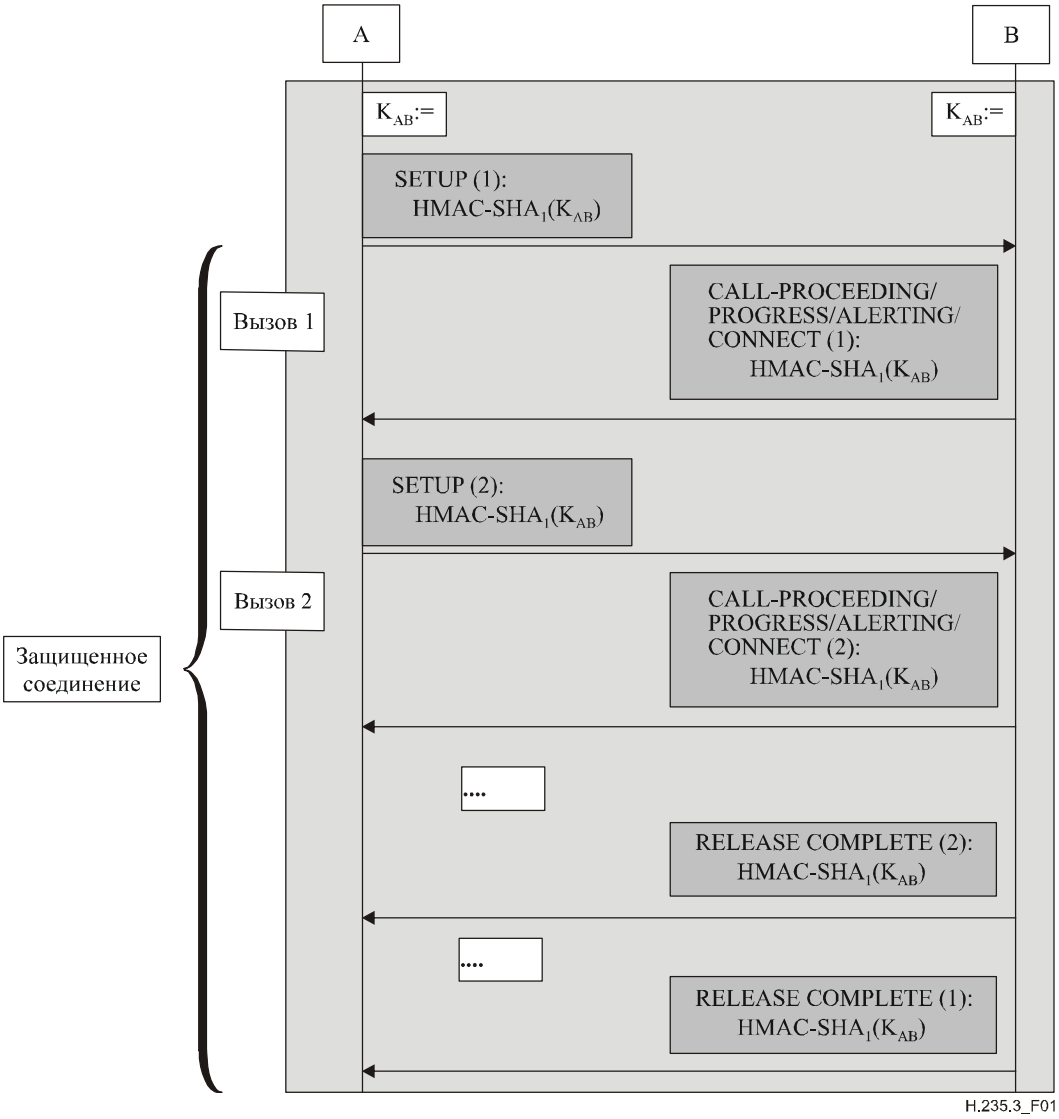


Рисунок 1/H.235.3 – Защищенное соединение для одновременных вызовов

9 Обновление ключа

Дополнительная процедура обновления ключа позволяет любому объекту связи (привратнику или оконечному устройству) обновить текущий сеансовый ключ на новый. Такое обновление ключа может быть инициировано нуждающимися в этом, какими угодно объектами. Обновление ключа может быть обусловлено скомпрометированным сеансовым ключом, предчувствием того, что сеансовый ключ является или может стать незащищенным или может быть выбран какой-либо другой критерий политики защиты.

Инициатор запрашивает обновление ключа, использующее сообщение FACILITY. Сообщение FACILITY для обновления ключа передает новый маркер Диффи-Хеллмана, дополнительный цифровой сертификат и цифровую подпись инициатора. Пока идет прием сообщения FACILITY, получатель отвечает похожим сообщением FACILITY, передающим маркер Диффи-Хеллмана, дополнительный цифровой сертификат и цифровую подпись получателя. Во время завершения процедуры обновления ключа, инициатор и ответчик должны использовать вычисленный новый ключ связи.

– маркер **tokenOID** маркера **ClearToken** внутри FACILITY должен быть установлен на "Q", что означает использование алгоритма Диффи-Хеллмана и гибридного профиля защиты. Вычисление сеансового ключа происходит по той же схеме, что и вычисление сеансового медиаключа (см. 8.5/H.235.6).

Сообщение FACILITY, используемое с целью обновления ключа, должно быть защищено согласно процедуре II H.235.2. Любые другие сообщения FACILITY, не передающие маркер Диффи-Хеллмана, не должны применяться с целью обновления ключа, такое сообщение FACILITY должны быть защищены согласно процедуре I пункта 7/H.235.1.

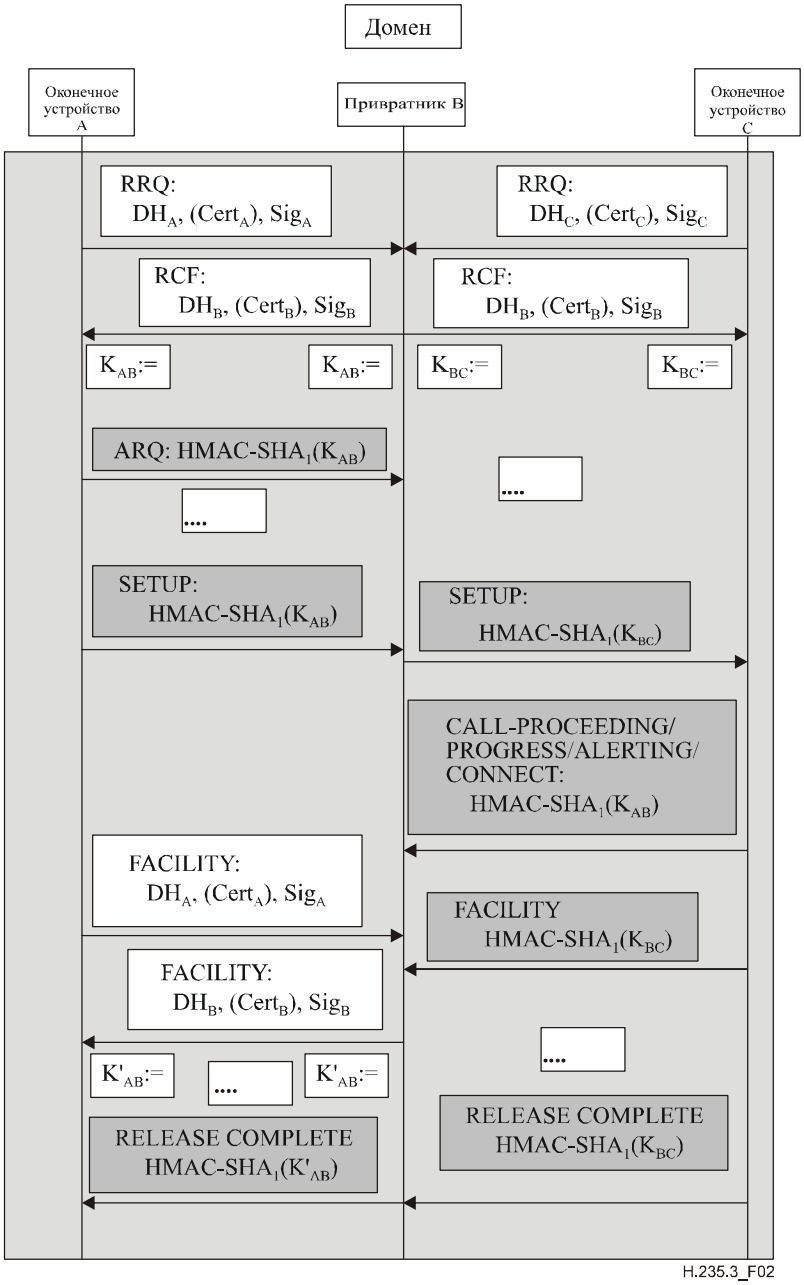
10 Использование метода эллиптических кривых

Данная тема является предметом дальнейшего изучения.

11 Поясняющие примеры

Структурные схемы на рисунках 2 и 3 поясняют использование данной Рекомендации в основном потоке сообщения. Заметьте, что диаграммы не показывают полный поток сообщения и что некоторые сообщения пропущены для простоты понимания. Сообщения, окрашенные светлым цветом, относятся к цифровому профилю H.235.2, в то время как, сообщения темного цвета относятся к базовому профилю H.235.1. На рисунках акцентируются (самые важные) части защиты каждого сообщения (маркеры H.235 CryptoTokens, Tokens), в то время как мелкие детали в рисунки не включены.

На рисунке 2 структурная схема поясняет основной поток сообщения в сценарии с одним привратником внутри домена с одним администратором. При условии, если сертификат привратника известен всем вовлеченным в процесс оконечным устройствам, а так же оконечные устройства знают сертификат привратника, то нет необходимости передавать сертификаты внутри в процессе процедуры регистрации.



Cert	Сертификат пользователя	K, K'	Симметричный ключ связи
DH_A	Поле Диффи-Хеллмана g^a mod p	Sig	Цифровая подпись
DH_B	Поле Диффи-Хеллмана g^b mod p		
EP	Конечная точка (оконечное устройство)		
GK	Привратник		

Рисунок 2/H.235.3 – Структурная схема в домене с одним администратором

ПРИМЕЧАНИЕ 1. – На рисунках 2 и 3 также содержится процедура быстрого старта, когда сообщения сигнализации вызова SETUP и CALL PROCEEDING/PROGRESS/ALERTING/CONNECT включают маркер быстрого старта (см. 1.7/H.323). Кроме того, режим не быстрого старта допускается согласно 7.3.1/H.323. На рисунке 2 также показана процедура обновления ключа с использованием FACILITY между оконечным устройством A и привратником B.

На рисунке 3 приведен пример потока сообщения в сценарии с различными административными доменами. Несмотря на то, что, гибридный профиль защиты применяется внутри каждого домена между оконечным устройством и привратником, как показано на рисунке 2, гибридный профиль защиты может быть также применен между обоими доменами в момент установления фазы вызова.

ПРИМЕЧАНИЕ 2. – В рисунок 3 не включены никакие элементы связи между границами (BE), а также ни одна связь между привратником с BE. На рисунке 3 также показана процедура обновления ключа с использованием FACILITY между обоими доменами.

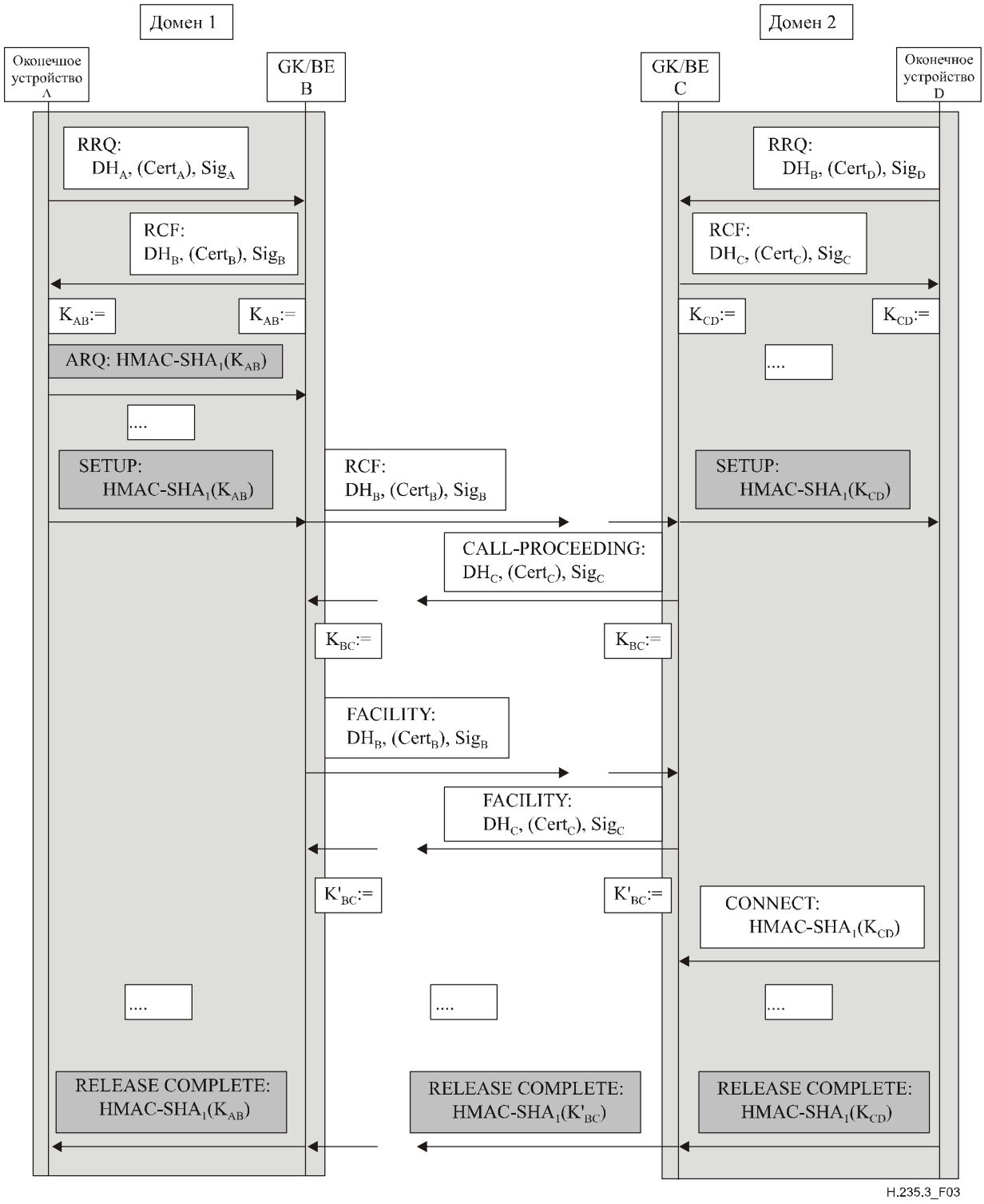


Рисунок 3/H.235.3 – Структурная схема в домене с многими администраторами

12 Многоадресный режим

Многоадресные сообщения H.225.0 такие, как **GRQ** или **LRQ**, должны включать **CryptoToken** согласно процедуре II, где **generalID** не установлено. Когда такие сообщения участвуют в одноадресной передаче, то сообщение должно включать **CryptoToken** с установленным **generalID**.

13 Список защищенных сообщений сигнализации

Как показано ниже, процедура IV использует процедуру I из H.235.1 или процедуру II из H.235.2, в зависимости от сценария и имеющегося сообщения.

13.1 Сообщения H.225.0 RAS

Сообщения H.225.0 RAS	Поля сигнализации H.235	Аутентификация и целостность	Неотказуемость
GatekeeperRequest, GatekeeperConfirm, GatekeeperReject, если применяется обнаружение привратника RegistrationRequest, RegistrationConfirm, RegistrationReject, если не применяется обнаружение привратника	CryptoToken, ClearToken	Процедура II	Процедура II
Любые другие сообщения RAS (Примечание 2)	CryptoToken	Процедура I	
ПРИМЕЧАНИЕ 1 – При одноадресной передаче сообщений, процедура II должна применяться с полями безопасности, использующими CryptoToken. ПРИМЕЧАНИЕ 2. – Обнаружение привратника и одноадресные сообщения не установлены.			

13.2 Сигнализация вызова (домен с одним администратором)

Сообщение сигнализации вызова H.225.0	Поля сигнализации H.235	Аутентификация и целостность	Неотказуемость
Setup-UUIE, Connect-UUIE (Примечание 1), Facility-UUIE (Примечание 2), Alerting-UUIE, CallProceeding-UUIE, Facility-UUIE, Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	CryptoToken, ClearToken	Процедура I	
Facility-UUIE (Примечание 3)	CryptoToken	Процедура II	Процедура II
ПРИМЕЧАНИЕ 1. – При условии, что и то, и другое сообщение является первым в каждом направлении. ПРИМЕЧАНИЕ 2. – Не используется для обновления ключа. ПРИМЕЧАНИЕ 3. – Используется для обновления ключа.			

13.3 Сигнализация вызова H.225.0 (домен со многими администраторами)

Сообщение сигнализации вызова H.225.0	Поля сигнализации H.235	Аутентификация и целостность	Неотказуемость
Setup-UUIE, Connect-UUIE (Примечание 1), Alerting-UUIE (Примечание 2), CallProceeding-UUIE, Facility-UUIE (Примечание 3), Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE	CryptoToken, ClearToken	Процедура II	Процедура II
Alerting-UUIE (Примечание 4), CallProceeding-UUIE, Facility-UUIE (Примечание 5), Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	CryptoToken, ClearToken	Процедура I	Процедура I
ПРИМЕЧАНИЕ 1. – При условии, что и то, и другое сообщение является первым в каждом направлении. ПРИМЕЧАНИЕ 2. – Любое из этих сообщений встречается как первое сообщение в каждом направлении. ПРИМЕЧАНИЕ 3. – Используется для обновления ключа ПРИМЕЧАНИЕ 4. – Любое из этих сообщений не встречается как первое сообщение в каждом направлении. ПРИМЕЧАНИЕ 5. – Не используется для обновления ключа			

14 Список идентификаторов объекта

В таблице 2 перечислены все упомянутые в данной Рекомендации OID (идентификаторы объекта).

Таблица 2/H.235.3 – Идентификаторы объекта

Обозначение идентификатора объекта	Значение (значения) идентификатора объекта	Описание
"A1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 20}	Используется как замена для OID "A" в процедуре II Рек. МСЭ-Т H.235.2 для CryptoToken-tokenOID, указывающая, что подпись RSA/хеш включает все поля в RAS H.225.0 или сообщения сигнализации вызова (аутентификация и целостность).
"S1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 21}	Используется как замена для OID "S" в процедуре II Рек. МСЭ-Т H.235.2 для ClearToken-tokenOID, указывающая, что ClearToken было использовано для аутентификации и целостности сообщения. Данный OID в сквозном CryptoToken неявно указывает, что во время быстрого старта также используется алгоритм Диффи-Хеллмана.
"Q"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 22}	Используется в процедуре IV, указывающей, что ClearToken в связи hop-by-hop несет маркер Диффи-Хеллмана.
"W"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 23}	Используется в процедуре IV как алгоритм OID, указывающий использование цифровой подписи, основанной на RSA SHA1.

Дополнение I

Процессор защиты привратника, допустимый H.235.3

В данном информационном Дополнении описывается пример реализации процессора защиты привратника (GKSP), допустимого H.235.3, в соединении с привратником. Целью GKSP является перенести некоторые конкретные задачи защиты H.235.3, такие, как выполнение дорогостоящих в исполнении операций Диффи-Хеллмана, вычисление и подтверждение цифровой подписи, а также обработку сертификата X.509 из единого привратника в новый и отдельный функциональный объект – процессор защиты привратника (GKSP). Существует, по меньшей мере, один объект GKSP для каждого привратника, еще один привратник также может управлять многочисленными GKSP, для того чтобы увеличить масштабируемость и число обслуживаемых конечных точек, а также улучшить устойчивость целых систем.

На рисунке I.1 показана такая разложенная на части структура привратника, где GKSP содержит функции защиты H.235.3.

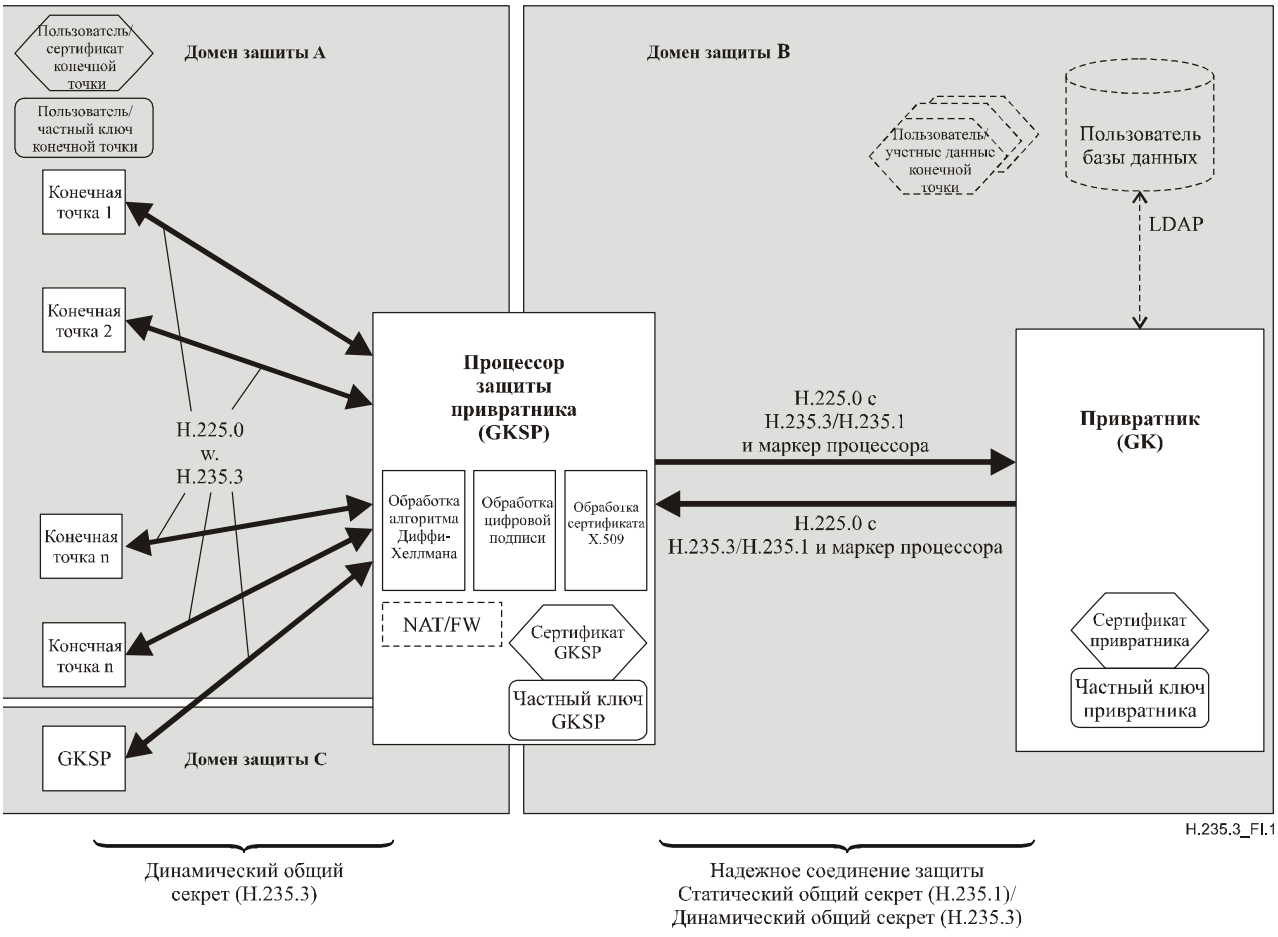


Рисунок I.1/H.235.3 – Структура процессора защиты привратника

ПРИМЕЧАНИЕ 1. – GKSP может содержать добавочные полезные функции, как, например, NAT (функция трансляции сетевых адресов), брандмауэр, шлюз уровня приложения (ALG) и т. д., такие функции могут быть частью процесса защиты или могут содержаться, как отдельные внутренние функции, тем не менее, такие функции не описываются в данном пункте и являются объектами для дальнейшего изучения.

GKSP управляет определенным числом конечных точек внутри административного домена защиты A. GKSP также может соединяться с другим GKSP в каком-либо другом административном домене защиты C (не показано).

ПРИМЕЧАНИЕ 2. – На практике, эти три административных домена защиты не обязательно должны быть отдельными. GKSP может быть размещен внутри административного домена B, где уже существует привратник, или в качестве альтернативы, GKSP может быть размещен внутри домена защиты A, или внутри отдельного, своего собственного домена защиты (не показано).

При использовании GKSP привратнику не потребуется участвовать в операциях по защите, требующих дорогостоящих компьютерных вычислений. Привратник все также определяет разрешение и доступ путем противопоставления соответствующих учетных данных (например, псевдоним/отличительное имя/порядковый номер сертификата/сертификат X.509) (внутренней/ внешней) базе данных, содержащей описания пользователей с их разрешениями и учетными данными. В пункте I.3 определяются соответствующие учетные данные для использования GKSP, допустимого H.235.3.

ПРИМЕЧАНИЕ 3. – Возможный интерфейс LDAP между привратником и абонентом/пользователем базы данных не является предметом рассмотрения в данной Рекомендации. Этот процесс оставлен на усмотрение политике привратника, по каким критериям и учетным данным (например, псевдоним/отличительное имя/порядковый номер сертификата) принимать решение управления доступом. Это остается на усмотрение той базе данных пользователя, чьи учетные данные (псевдоним/отличительное имя/порядковый номер сертификата) там хранятся.

ПРИМЕЧАНИЕ 4. – У GKSP нет необходимости участвовать в любых вопросах относительно конфигурации или администрации пользователей или абонентов, а также GKSP не нужно иметь доступ к базе данных пользователя.

ПРИМЕЧАНИЕ 5. – Конечные точки, применяемые H.235.3, и GKSP также обычно содержатся в корневом сертификате (не показано на рисунке 1). Корневой сертификат позволяет объекту проверять сертификат объекта (EP, GKSP).

Связь между GKSP и его GK, или между двумя GKSP является защищенной. Например, H.235.1 используется, когда применяется статически сформированный общий секрет. Применение H.235.2 позволяет устанавливать динамический общий секрет. И в том, и в другом случае GK и GKSP допускают наличие установленной общей, надежной взаимосвязи, а также могут быть либо в статическом соединении защиты, либо в динамическом соединении защиты. Доверительная взаимосвязь может передаваться по цепочке от одного GKSP к следующему, в случае, когда используется множество GKSP.

Таким образом, GK доверяет GKSP выполнение процедур аутентификации на дальнем конце линии связи и текущее осуществление процедур защиты. GKSP сообщает GK результат защитной обработки в простом утверждении о защите, используя маркер процессора.

Предполагается, что каждая конечная точка, допустимая в соответствии с H.235.3, и GKSP содержат сертификат X.509, который достоверно связывает идентичность законного владельца открытого ключа и соответствующий частный ключ для подписи.

ПРИМЕЧАНИЕ 6. – Открытый ключ, соответствующий частному ключу не показан детально на рисунке I.1; обычно, подтвержденный открытый ключ передается внутри пользователя X.509 /сертификата конечной точки.

ПРИМЕЧАНИЕ 7. – Показаны не все сертификаты/частные ключи для всех конечных точек/GKSP.

ПРИМЕЧАНИЕ 8. – Сертификат GKSP это, обычно, сертификат сервера.

GK должен содержать в себе индивидуальный, однозначный сертификат GK и частный ключ только в случае, если GK для связи с GKSP применяет H.235.3.

GKSP – это устойчивый модуль доступа, действующий в интервалах между конечными точками и GK, или в интервалах между двумя привратниками. Существует по меньшей мере один объект GKSP для каждого привратника, еще один привратник также может управлять многочисленными GKSP, для того чтобы увеличить масштабируемость и число обслуживаемых конечных точек, а также улучшить устойчивость единых систем. Элементы GKSP, определенные H.235.3, можно классифицировать в виде линейной цепочки, как показано на рисунке I.2. Элементы GKSP, определенные H.235.3, можно классифицировать в виде иерархической структуры, как показано на рисунке I.3.

Существует, по крайней мере, один общий объект GKSP для каждого GK, еще один привратник также может управлять многочисленными общими GKSP, для того чтобы увеличить масштабируемость и число обслуживаемых конечных точек, а также улучшить устойчивость единых

систем. Это может быть один или более общих GKSP между конечной точкой и GK: так, для некоторых GKSP, в принципе, может быть возможна линейная или иерархическая, каскадная конфигурация. Конечная точка обычно устанавливает доверительную связь со связанным с ней GK через один или более GKSP. Один GK может иметь множественные доверительные взаимосвязи со множественными конечными точками.

На рисунке I.2 показана структура с линейно цепочными элементами GKSP.

Рисунок I.2/H.235.3 – Цепочная структура GKSP

На рисунке I.2, GKSP1 аутентифицирует сообщение RRQ полученное от EP1, в то время как, GK1 и GK2 принимают решение об авторизации EP1. GKSP1, GKSP2 (соответственно GKSP3 и GKSP4) полагаются на сообщения сигнализации H.235.3 между EP1 и GK1 (соответственно, GK1 и GK2).

На рисунке I.3 показана структура с иерархическими, каскадными элементами GKSP.

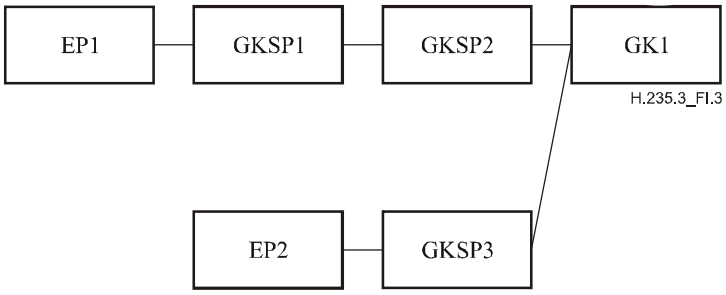


Рисунок I.3/H.235.3 – Иерархическая структура GKSP

GKSP имеет, по крайней мере, один адрес IP, обычно, GKSP представляет собой краевое устройство защиты, которое располагается на границе двух отдельных административных доменов защиты. Таким образом, GKSP может владеть двумя адресами IP, один адрес IP по отношение к конечным точкам /равноправным GKSP (административные домены защиты A и C), и еще один внутренний адрес IP – для GK (административный домен защиты B).

I.1 Обнаружение процессора защиты привратника

Предполагается, что конечная точка H.235.3 не должна знать о присутствии GKSP. Конечная точка может иметь сконфигурированный адрес IP GKSP, в качестве контактной точки GK. В сценарии с присутствием привратника, конечная точка работает точно также, как и в сценарии без использования GKSP. Конечная точка может использовать фазу обнаружения GK, используя **GRQ** для размещения обслуживающего ее (конечную точку) GKSP.

В случае когда существует GKSP, который обслуживает запрашиваемую конечную точку, GKSP необходимо выяснить, поддерживается ли принадлежащий ему GK процессором защиты.

В случае когда GKSP намеревается использовать H.235.1 по отношению к GK, но общий секрет еще не сконфигурирован между GKSP и GK, то B GKSP возвращает **GRJ** на конечную точку с причиной **reason**, установленной на **securityDenial**/**securityDenied**. В противном случае, GKSP направляет **GRJ**, включает процессор ClearToken и устанавливает значение элемента профиля на ID 0, как определено в таблице I.1. С того момента как, в данном случае, GK поддерживает GKSP, GK возвращает **GCF**/**GRJ** и включает маркер процессора.

В случае когда GKSP намеревается использовать H.235.3 по отношению к GK, GKSP направляет **GRQ** в GK включением процессора ClearToken, и устанавливает значение элемент профиля на ID 0, как определено в таблице I.1. GK с допустимым GKSP, поддерживающим данное Дополнение, отвечает сообщением **GCF** и включает процессор ClearToken.

GK, который не поддерживает процессор защиты или GK, в котором не обеспечивается выполнение данного Дополнения, мог бы игнорировать передаваемый маркер процессора и мог бы ответить

GCF/**GRJ**. GKSP способен распознавать такую ситуацию, когда полученное **GRQ/GRJ** не передает маркер процессора. GKSP затем отправляет **GRJ** на конечную точку с причиной **reason**, установленной в **securityDenial**/**securityDenied**.

GK, который получил сообщение **GRQ** непосредственно от конечной точки, без трансляции его через GKSP, и когда GK осведомлен о наличии GKSP, то GK отвечает **GRJ** с причиной **reason**, установленной на **securityDenial**/**securityDenied** (без включения маркера процессора).

I.2 Функционирование процессора защиты привратника

Процессор защиты привратника выполняет, по крайней мере, следующие функции:

– Завершает протокол H.235.3 к конечным точками H.235.3, или к равноправным GKSP, как определено в процедуре IV.

– Запускает протокол Диффи-Хеллмана H.235.3 по направлению к конечным точкам H.323/равноправному GKSP, например, выполняет модульно-экспоненциальные операции Диффи-Хеллмана.

– Выполняет проверку цифровых подписей, полученных от конечных точек H.323 или равноправного GKSP в защищенных сообщениях H.235.3.

– Безопасность контролируется полученными цифровыми сертификатами X.509: проверка пути, контроль истинности, контроль списка аннулированных сертификатов (CRL), и т. д.

– Для сообщений, перенаправляемых от GKSP к GK или к другому GKSP, GKSP генерирует новые маркеры H.235 (H.235.1 или H.235.3). В базовом ClearToken H.235, GKSP использует идентификатор GKSP в качестве **sendersID**, а идентификатор привратника (GKID) в качестве **generalID**.

– Для сообщений, полученных от конечной точки H.235.3, В GKSP включает маркер процессора. Для исходного сообщения **RRQ**/**GRQ** маркер процессора содержит элемент профиля защиты с ElementID 0, что указывает на обнаруженный метод аутентификации. GKSP может включать элемент профиля с ElementID 0 в любом другом RAS H.225.0 и /или также в сообщении Сигнализации вызова.

Более того, маркер процессора содержит один или несколько элементов профиля защиты, которые передают учетные данные.

Подходящими учетными данными, используемыми в контексте данного Дополнения, являются:

– ElementID 1 для предоставления субъекта, находящегося в сертификате X.509.

– ElementID 2 для предоставления subjectAltName, находящегося в сертификате X.509.

– ElementID 3 для предоставления порядкового номера, находящегося в сертификате X.509.

– ElementID 4 для предоставления имени запрашивающей стороны, находящейся в сертификате X.509.

– ElementID 5 для предоставления идентификатора конечной точки оконечного устройства H.323.

ПРИМЕЧАНИЕ. – GK может дополнительно интерпретировать элемент псевдонима H.323 в сообщениях H.225.0 в качестве учетных данных. С того момента, как элемент псевдонима, так или иначе, присутствует в сообщениях, нет необходимости определять отдельный элемент псевдонима внутри элемента профиля защиты.

GKSP также включает элемент профиля защиты с ElementID 6, указывающий на обнаруженную ошибку. Если аутентификация между конечной точкой H.323 и GKSP прошла успешно, то затем GKSP может включить элемент профиля защиты с ElementID 6, для того чтобы указать, что ошибки защиты обнаружено не было.

– В случае когда GKSP обнаруживает ошибки защиты (неверная цифровая подпись, поврежден сертификат истинности и т. д.) в сообщении, полученном от конечной точки H.323 или от равноправного GKSP, GKSP записывает ошибку и направляет сообщение привратнику, включает маркер процессора с элементом профиля защиты типа ElementID 6, указывающим тип ошибки, и предоставляет привратнику право решать и реагировать соответственно.

– В случае когда GKSP встречает ошибки защиты в сообщении, полученном от GK или от другого GKSP, GKSP записывает ошибку и отклоняет сообщение.

– Вычисляет цифровые подписи для выходящих сообщений H.235.3 к конечным точкам H.323 или равноправному GKSP.

– Транслирует любые сообщения H.225.0 между конечной точкой H.323 и привратником или GKSP туда и обратно и выполняет следующие операции в маркерах:

  • Обменивается данными со своим привратником, используя протокол H.225.0, в котором маркеры H.235.3, полученные от конечной точки H.323 или от равноправного GKSP в первом сеансе квитирования, очищены.

  • Проверяет вложенные маркеры H.235.1, полученные от конечных точек H.323 или от равноправного GKSP, и очищает их для дальнейшей трансляции сообщения к привратнику.

  • Завершает протокол H.235.1/H.235 к своему привратнику.

  • Включает маркеры H.235.1/H.235.3 для выходящих сообщений применительно к конечным точкам H.323 или по отношению к равноправному GKSP.

  • Оставляет полученные сообщения H.225.0, полученные от конечных точек H.323 или GK, в основном, нетронутыми, только переписывает маркеры, как это определено выше.

  • Протокол H.225.0 между GKSP и его GK защищается с применением или базового профиля защиты H.235.1 или гибридного профиля защиты H.235.3.

– В случае когда GKSP и GK или GKSP и другой GKSP применяют гибридный профиль защиты H.235.3, GKSP либо:

  a) запускает протокол H.235.3 применительно к GK или GKSP для установления нового динамического ключа для приема первого сообщения от первой конечной точки или равноправного GKSP; либо

  b) инициирует протокол H.235.3 применительно к GK или GKSP для установления нового динамического ключа до того, как любая другая конечная точка H.323 или равноправный GKSP начнут обмениваться данными. Это позволит динамическому общему секрету находиться на месте, готовым к применению, для того чтобы защитить сообщения, полученные при первом сеансе квитирования от устройства H.323 или равноправного привратника, это может способствовать уменьшению общего времени установки безопасного соединения.

– GKSP не пересылает сообщения FACILITY, характерные для H.323, для обновления ключа.

– В случае когда GKSP и GK или GKSP и другой GKSP используют базовый профиль защиты H.235.1, GKSP применяет статический общий ключ для защиты RAS H.225.0 и /или сообщений сигнализации вызова.

– Отслеживает соединения защиты, например, устанавливает общий секрет Диффи-Хеллмана; поддерживает динамические общие секреты. В зависимости от политики защиты, GKSP может запускать смену шифровальных ключей для поддерживаемого динамического общего секрета (секретов), используя сообщения FACILITY. Если хотя бы однажды оконечное устройство H.323 или равноправный GKSP были лишены регистрации, GKSP следует отклонить динамический общий ключ и принять во внимание, что в данном месте нет безопасного соединения.

– Отображает транспортные порты (EP-GKSP и GKSP-GK) для RAS H.225.0 и /или сигнализации вызова протоколов “один к одному”.

I.3 Маркер процессора

Во время приема защищенного H.235.3 сообщения RAS H.225.0 и /или сообщения Сигнализации вызова с передаваемым сертификатом X.509 и цифровой подписью, GKSP перемещает маркеры H.235.3 и включает отдельный маркер процессора в сообщение перенаправленное GK или следующему GKSP (если GKSP существует).

Вместе с маркером процессора, GKSP сообщает обнаруженный метод аутентификации, обнаруженный идентификатор объекта, обнаруженное имя в сертификате (имя или subjectAltName), обнаруженный порядковый номер в сертификате X.509, обнаруженное имя запрашивающей стороны в сертификате X.509 или указание на ошибку. Маркер процессора выполняет роль простого

утверждения защиты, показывающего утвержденную защитную взаимосвязь (успешно или сбой) между GKSP и конечными точками H.323 применительно к GK.

GK способен обнаруживать присутствие GKSP, путем изучения полученного сообщения и распознавания включенного поля процессора. GK интерпретирует, что отсутствие любого маркера процессора указывает на отсутствие какого-либо GKSP.

Маркер процессора обозначается ClearToken, в нем используются следующие поля:

– **tokenOID** содержит OID для "PT", см. таблицу I.2.

– **generalID** содержит либо:

  • идентификатор EP конечной точки H.323 в случае, если защищенное сообщение H.235 получено от конечной точки H.323, либо;

  • идентификатор GK, в случае, если защищенное сообщение H.235 получено от GK.

– **certificate** дополнительно может содержать полученный сертификат H.235.2/H.235.3, полученный от конечной точки H.323 или равноправного GKSP. Если указанная функция осуществляется, то GKSP пересылает сертификат GK.

  Применение subject/subjectAltName,или конечной точки ID, или порядкового номера сертификата, или легкодоступных учетных данных, является более предпочтительным, чем использование целого сертификата внутри поля **certificate**. Это объясняется тем, что, во первых, сертификаты X.509 занимают слишком большую часть данных и, во-вторых, из-за потенциальных проблем с фрагментацией сообщения, когда сертификаты включаются в UDP-транспортировку сообщений H.225.0.

– **profileInfo** содержит, по крайней мере, один элемент профиля.

  Маркер процессора может содержать несколько элементов профиля, из тех, которые перечислены в таблице I.1:

Все остальные поля внутри процессора защиты GK остаются неиспользованными.

Таблица I.1/H.235.3 – Спецификация элементов профиля

Значение ElementID	Описание	Спецификация
0	Указывает элемент профиля, который передает метод аутентификации. Использование этого элемента профиля является обязательным для начального сеанса квитирования (GRQ или RRQ) и необязательным во всех остальных случаях.	• **ParamS** остается неиспользованным. • **Element** содержит элемент, в котором **integer** установлено на одно из следующих значений, указывающий обнаруженный метод аутентификации в конечной точке H.323 или равноправном GKSP: 1) другой, точно не установленный и нестандартный метод аутентификации; 2) никакой (например, нет аутентификации); 3) общий секрет H.235.1 (не определен в данном Дополнении); 4) H.235.2; 5) H.235.3; 6) H.235.5 (не определен в данном Дополнении); 7) H.235.4 (не определен в данном Дополнении); 8) H.530 (не определен в данном Дополнении).

Таблица I.1/H.235.3 – Спецификация элементов профиля

Значение ElementID	Описание	Спецификация
1	Указывает элемент профиля, который содержит **subject** полученного сертификата. Использование этого элемента профиля является необязательным.	• **ParamS** остается неиспользованным. • **Element** содержит Element, в котором **name** или **octets** содержит **subject** полученного сертификата. ПРИМЕЧАНИЕ. – GKSP может быть необходимо перекодировать **subjectAltName** из представления Name X.509 в строку **octets** или **name** в BMP формате.
2	Указывает элемент профиля, который содержит **subjectAltName** полученного сертификата. Использование этого элемента профиля является необязательным.	• **ParamS** остается неиспользованным. • **Element** содержит Element, в котором **name** или **octets** содержит **subjectAltName** полученного сертификата. ПРИМЕЧАНИЕ. – GKSP может быть необходимо перекодировать **subjectAltName** из представления Name X.509 в строку **octets** или **name** в BMP формате.
3	Указывает элемент профиля, который содержит порядковый номер сертификата. Использование этого элемента профиля является обязательным.	• **paramS** остается неиспользованным. • **element** содержит Element, в котором **integer** содержит **CertificateSerialNumber** полученного сертификата X.509.
4	Указывает элемент профиля, который содержит имя запрашиваемого сертификата. Использование этого элемента профиля является обязательным.	• **paramS** остается неиспользованным. • **element** содержит Element, в котором **name** или **octets** содержит имя **issuer** полученного сертификата X.509. ПРИМЕЧАНИЕ. – GKSP может быть необходимо перекодировать имя **issuer** из представления Name X.509 в строку **octets** или **name** в BMP формате.
5	Указывает элемент профиля, который содержит конечную точку ID исходящей конечной точки /оконечного устройства. Использование этого элемента профиля является необязательным.	• **paramS** остается неиспользованным. • **element** содержит Element, в котором **name** содержит конечную точку идентификатора объекта исходящей конечной точки/оконечного устройства.
6	Указывает элемент профиля, который содержит обозначение ошибки. Использование этого элемента профиля является обязательным в случае, если присутствует ошибка ((> 0), и необязательным, в случае отсутствия ошибки (0).	• **paramS остается неиспользованным**. • **element содержит Element, в котором integer содержит одно из следующих зашифрованных обозначений ошибки**: 0: отсутствие ошибки 1: securityDenied 2: securityWrongSyncTime 3: securityReplay 4: securityWrongGeneralID 5: securityWrongSendersID 6: securityMessageIntegrityFailed 7: securityWrongOID 8: securityDHmismatch 9: securityCertificateExpired 10: securityCertificateDateInvalid

Таблица I.1/H.235.3 – Спецификация элементов профиля

Значение ElementID	Описание	Спецификация
		11: securityCertificateRevoked 12: securityCertificateNotReadable 13: securityCertificateSignatureInvalid 14: securityCertificateMissing 15: securityCertificateIncomplete 16: securityUnsupportedCertificateAlgOID 17: securityUnknownCA 18: неопределенная ошибка защиты 19: GKSP не поддерживается.

I.4 Пример иллюстрации GKSP

В данном пункте представлены структурные схемы сообщений (см. рисунки I.4 и I.5) для процессора защиты GK, функционирующего внутри административного домена защиты. Заметьте, что рисунки I.4 и I.5 показывают только те сообщения, которые являются наиболее значительными для H.235.3, на практике, может быть намного больше сообщений RAS H.225.0 и/или сообщений Сигнализации вызова.

На обоих рисунках оконечное устройство A, допустимое в соответствии с H.235.3, и GKSP используют гибридный профиль защиты H.235.3, таким образом, оконечное устройство A и B GKSP не используют совместно какой-либо статический общий секрет. На рисунке I.4 GKSP и GK применяют базовый профиль защиты для защиты сообщений RAS H.225.0 и сообщений Сигнализации вызова. K_{BC} представляет собой статический общий секрет, который используется совместно B GKSP и C GK.

На рисунке I.4 показан полный вызов из оконечного устройства A через B GKSP и C GK. В данном вызове используется GK-маршрутизация. В начале, в период регистрации RAS, оконечное устройство A и GKSP формируют динамический ключ связи K_{AB} согласно H.235.3. Для этого, оконечное устройство A генерирует сообщение **RRQ**, которое передает половину ключа Диффи-Хеллмана DH_A A, содержащий сертификат A (необязательно), и цифровую подпись A, сгенерированное сообщение **RRQ** передается целиком все или частями.

GKSP получает **RRQ** и проверяет цифровую подпись. Это включает в себя проверку достоверности и сверку переданного цифрового сертификата X.509 (если он включен) с корневым сертификатом оконечного устройства A, проверку CRL и т. д.

GKSP пересылает сообщение **RRQ** к C GK, добавляет маркер процессора (PT), включающего элементы профиля защиты:

– 0, указывающий на H.235.3 (5);

– 2, содержащий subjectAltName сертификата A;

– 3, порядковый номер сертификата A;

– 5, идентификатор конечной точки A,

и применяет базовый профиль защиты H.235.1 с общим ключом K_{BC}; контроль целостности вычисляется либо в целом сообщении **RRQ**, либо только в его определенных частях.

В случае если проверка достоверности сертификата или проверка достоверности цифровой подписи является неудовлетворительной, то B GKSP не может аутентифицировать и авторизовать оконечное устройство A, тогда GKSP регистрирует ошибку и пересылает неправильное RRQ к C GK.

Привратник C получает сообщение **RRQ**, проверяет контроль целостности путем применения K_{BC} и обрабатывает маркер процессора PT с включенными элементами профиля. Если C GK способен успешно подтвердить правильность **RRQ**, то C GK авторизует оконечное устройство A. После этого C GK отвечает сообщением **RCF**, которое посылается B GKSP.

B GKSP получает **RCF**, узнает, что C GK успешно авторизовал оконечное устройство A и посылает **RCF** оконечному устройству A путем вычисления и включения неполного ключа Диффи-Хеллмана DH_B, его сертификата (необязательно) и присваивает **RRQ** (полностью или частично) частный ключ. Оконечное устройство A подтверждает подлинность полученного сообщения **RCF**.

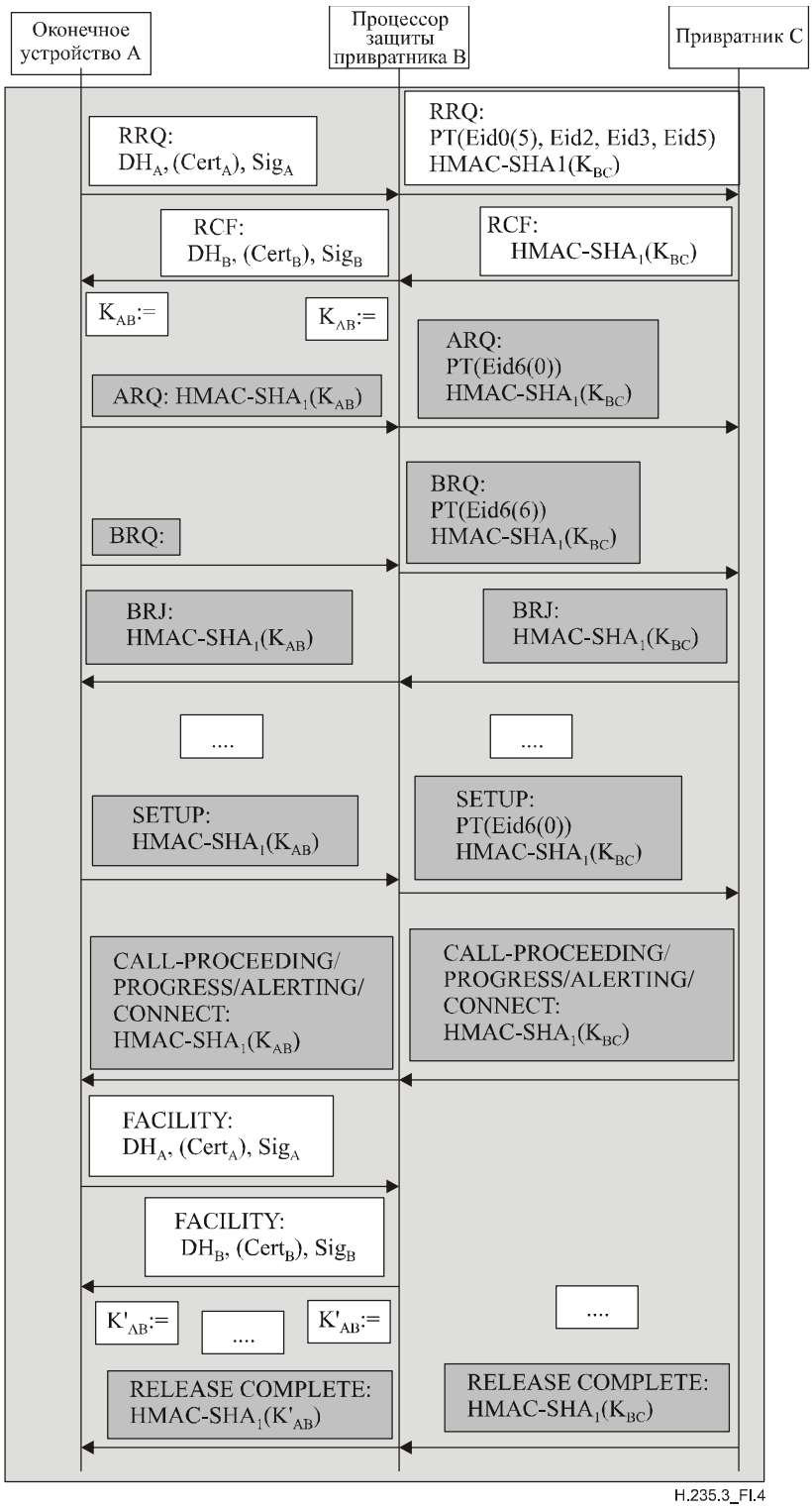
В случае когда B GKSP успешно аутентифицирует и авторизует оконечное устройство A, B GKSP и оконечное устройство A вычисляют динамический общий секрет K_{AB}. Этот динамический общий секрет представляет собой установленную надежную взаимосвязь между оконечным устройством A и B GKSP. Во всех других случаях, и в случае, где C GK не авторизует оконечное устройство A, B GKSP посылает **RCF** оконечному устройству A, путем вычисления и включения половины ключа Диффи-Хеллмана DH_B, его сертификата (необязательно) и присваивает **RRQ** (полностью или частично) частный ключ. С того момента, как оконечное устройство не является авторизованным, GKSPB больше не хранит $K_{AB.}$ B GKSP может записать поврежденное **RCF** в журнал регистрации.

Оконечное устройство A и B GKSP используют этот динамический общий секрет K_{AB} для дальнейшей защиты сообщений RAS H.225.0 и сообщений Сигнализации вызова, используя базовый профиль защиты H.235.1. B GKSP и C GK используют базовый профиль защиты H.235.1 для защиты всех сообщений RAS H.225.0 и всех сообщений Сигнализации вызова.

В случае когда оконечное устройство получает **RCF**, оконечное устройство A не продолжает установку вызова.

На рисунке I.4 также показан случай ошибки, когда оконечное устройство A (или кто-то другой) посылает GKSP незащищенное сообщение **BRQ**, такое сообщение может также возникнуть вследствие атаки, где атакующий каким-то образом устранил или обошел защиту безопасности H.235.1. GKSP обнаруживает неудавшуюся проверку целостности и пересылает сообщение **BRQ**, включающее маркер процессора GK, тогда как элемент профиля защиты указывает securityMessageIntegrityFailed (6). GK распознает нарушение защиты и не авторизует запрос ширины полосы пропускания путем отказа с ответом **BRJ**.

В некоторой момент, через какое-то время после установки вызова, оконечное устройство A принимает решение обновить ключ K_{AB}, путем выполнения процедуры обновления ключа для K_{AB} с B GKSP, K'_{AB} представляет собой новый обновленный ключ. В конце вызова это завершается C GK.



Cert	Сертификат пользователя	GKSP	Процессор защиты привратника
DH_A	Поле Диффи-Хеллмана g^a mod p	HMAC-SHA1	Вычисленное контрольное число целостности
DH_B	Поле Диффи-Хеллмана g^b mod p	K, K'	Симметричный ключ связи
Eid*n*	Профиль защиты ElementID со значением *n*	PT	Маркер процессора
EP	Конечная точка (оконечное устройство)	Sig	Цифровая подпись
GK	Привратник		

Рисунок I.4/H.235.3 – Структура вызова с процессором GK-защиты и защита сообщения H.235.1 (из B GKSP к GK)

На рисунке I.5 GKSP и GK применяют гибридный профиль защиты H.235.3 для защиты сообщений RAS H.225.0 и сообщений Сигнализации вызова. K_{BC} представляет собой динамический общий секрет, который GKSP и GK сформировывают и дальше используют совместно внутри базового профиля защиты H.235.1 для защиты сообщений RAS H.225.0 и сообщений Сигнализации вызова. На рисунке I.5 также изображено оконечное устройство D, допустимое H.235.1, в котором используется совместно с B GKSP статический общий секрет $K_{DB.}$

На рисунке I.5 показан вызов в целом из оконечного устройства A через B GKSP и C GK. B данном вызове используется GK-маршрутизация. На рисунке I.5 предполагается, что оконечное устройство A в действительности является первой конечной точкой, которая регистрируется в GK через GKSP.

Оконечной устройство A и B GKSP используют этот динамический общий секрет K_{AB}, чтобы защитить дальнейшие сообщения RAS H.225.0 и сообщения Сигнализации вызова, которые используют базовый профиль защиты H.235.1. B GKSP и C GK используют базовый профиль защиты H.235.1 для защиты дальнейших сообщений RAS H.225.0 и сообщений Сигнализации вызова, использующих динамический общий секрет $K_{BC.}$

Вначале оконечное устройство A и B GKSP формируют динамический ключ связи $K_{AB,}$ согласно H.235.3. Во время первого сеанса обмена с квитированием **RRQ**/**RCF** между оконечным устройством A и GKSP, где в обоих объектах установлен динамический общий секрет K_{AB}, GKSP и GK также применяют H.235.3 для установления динамического общего секрета $K_{BC.}$

GKSP пересылает сообщение **RRQ**, полученное от оконечного устройства A, добавляет маркер процессора, включающий три элемента профиля защиты:

– 0, указывающий на H.235.3 (5);

– 3, порядковый номер сертификата A;

– 6, указывающий на отсутствие ошибок (0),

и применяет гибридный профиль защиты H.235.3. C того момента, как B GKSP и C GK больше не используют совместно какой-либо общий секрет, GKSP и GK запускают протокол H.235.3 и устанавливают динамический общий секрет $K_{BC.}$

Некоторое время спустя оконечное устройство D регистрируется в B GKSP, используя **RRQ**, защищенное H.235.1. B GKSP перенаправляет сообщение **RRQ** в C GK и включает маркер процессора. Маркер процессора предает три элемента профиля защиты:

– 0, указывающий на H.235.1 (3);

– 5, обслуживающий идентификатор конечной точки D;

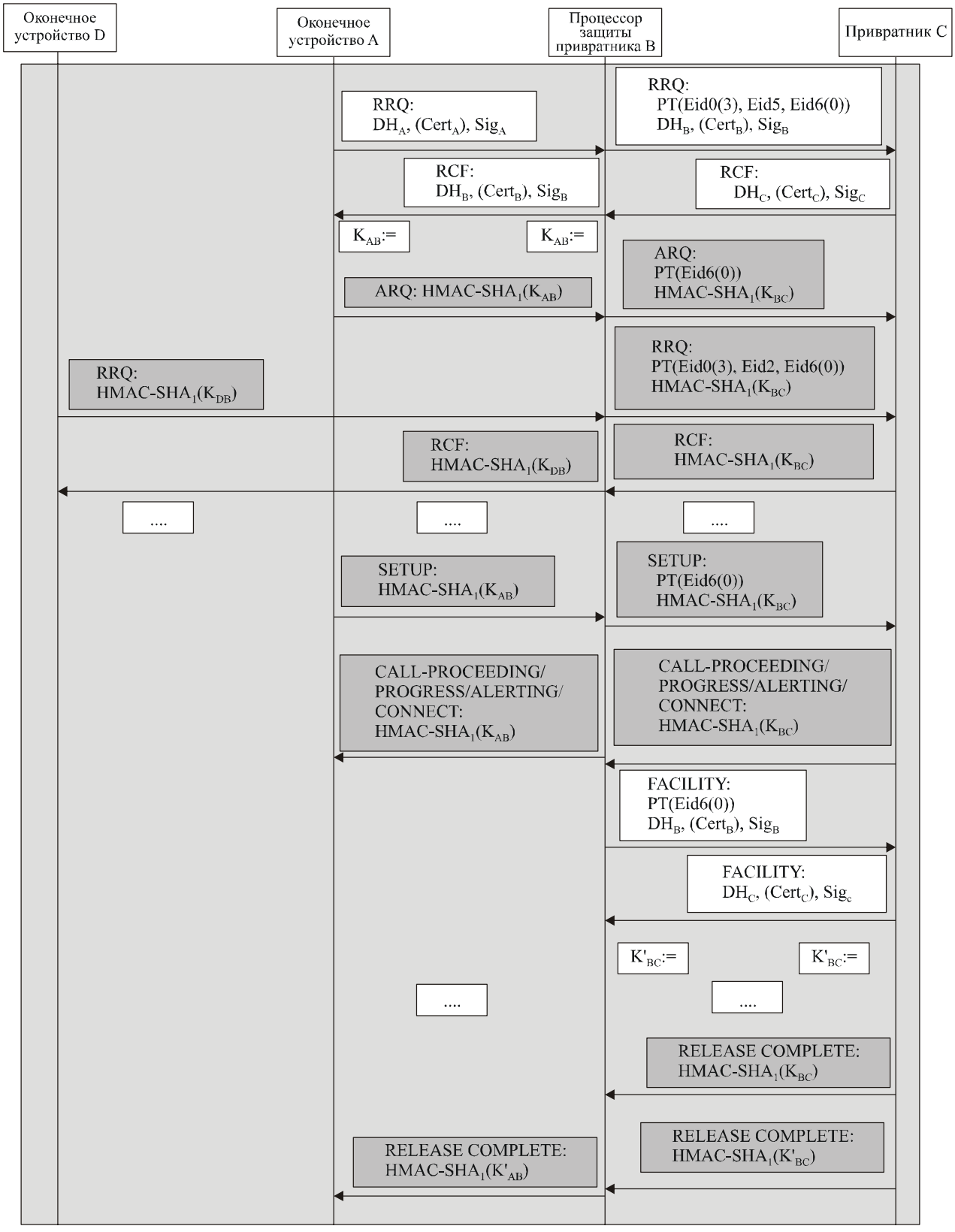
– 6, указывающий на отсутствие ошибок (0),

и применяет гибридный профиль защиты H.235.3. До того момента, пока еще не установлен динамический общий секрет K_{BC} H.235.3, GKSP защищает пересылаемые сообщения **RRQ**, используя H.235.1, применяя K_{BC}. C GK авторизует оконечное устройство D и отвечает сообщением **RCF**, которое GKSP пересылает в оконечное устройство D.

B некоторой момент времени после того, как запрос от оконечного устройства A в C Gkбыл установлен, B GKSP принимает решение обновить ключ K_{BC}, путем выполнения процедуры обновления ключа для K_{BC} с C GK, K'_{BC} представляет собой новый обновленный ключ.

На рисунке I.5 также изображен случай ошибки, когда GKSP получает от GK сообщение RELEASE-COMPLETE. B GKSP определяет, что нарушена проверка целостности; это сообщение не использует текущий ключ. Сообщение могло быть воспроизведено или подделано атакующим или GK, использующим устаревший и недействующий ключ. B GKSP записывает событие защиты и отклоняет сообщение, не пересылая его в оконечное устройство A.

B конце вызова это завершается C GK.



H.235.3_FI.5

Cert	Сертификат пользователя	GK	Привратник
DH_A	Маркер Диффи-Хеллмана g^a_b mod p	GKSP	Процессор защиты привратника
DH_B	Маркер Диффи-Хеллмана g^b_c mod p	HMAC-SHA1	Вычисленное контрольное значение целостности
DH_C	Маркер Диффи-Хеллмана g^c mod p	K, K'	Симметричный ключ связи
Eid*n*	Профиль защиты ElementID со значением *n*	PT	Маркер процессора
EP	Конечная точка (оконечное устройство)	Sig	Цифровая подпись

Рисунок I.5/H.235.3 – Структура вызова с процессором GK-защиты и защита сообщения H.235.3 (из B GKSP GK)

I.5 Список идентификаторов объекта

В таблице I.2 перечислены использованные OID, таблицу I.2 и таблицу I.1 следует использовать совместно.

Таблица I.2/H.235.3 – Идентификаторы объекта, используемые в Дополнении I

Обозначение идентификатора объекта	Значение (значения) идентификатора объекта	Описание
"PT"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 15}	Используется для указания маркера процессора GK Clear token при передаче информации от GKSP к GK.

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.