МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т J.125

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(04/2004)

СЕРИЯ J: КАБЕЛЬНЫЕ СЕТИ И ПЕРЕДАЧА СИГНАЛОВ ТЕЛЕВИЗИОННЫХ И ЗВУКОВЫХ ПРОГРАММ И ДРУГИХ МУЛЬТИМЕДИЙНЫХ СИГНАЛОВ

Интерактивные системы для распределения цифрового телевидения

Защита персональной информации в звене связи с кабельными модемами

Рекомендация МСЭ-Т J.125

Рекомендация МСЭ-Т J.125

Защита персональной информации в звене связи с кабельными модемами

Резюме

Данная Рекомендация была Приложением O к Приложению B Рек. J.112. Поскольку это Приложение применимо также к услугам защиты уровня MAC для Рек. МСЭ-Т J.122, оно стало самостоятельной Рекомендацией (J.125). Эта Рекомендация, которую часто относят к интерфейсу базовой защиты плюс или BPI+, преследует следующие две цели:

- обеспечить пользователям кабельных модемов защиту данных в кабельной сети, и
- обеспечить операторам кабельной сети защиту этой услуги, т. е. предотвратить доступ несанкционированных пользователей к сетевым службам RF MAC.

Интерфейс BPI+ обеспечивает в общей среде передачи кабельной сети уровень защиты данных равный или лучше, чем уровень, который обеспечивают предназначенные для этого службы доступа к сети (аналоговые модемы или цифровые абонентские линии).

Источник

Рекомендация МСЭ-Т J.125 утверждена 22 апреля 2004 года 9-й Исследовательской комиссией МСЭ-Т (2001–2004 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

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.

Всемирная ассамблея по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяет 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 соответствие 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 то, 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 реализации этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т J.125

Защита персональной информации в звене связи с кабельными модемами

1 Область применения

Эта Рекомендация обеспечивает возможность услуг защиты уровня MAC (шифрование и идентификацию) для связи транспортной службы CMTS-CM DOCSIS. Эта Рекомендация, которую часто относят к интерфейсу базовой защиты плюс, или BPI+, преследует следующие две цели:

- обеспечить пользователям кабельных модемов защиту данных в кабельной сети, и
- обеспечить операторам кабельной сети защиту этой услуги, т. е. предотвратить доступ несанкционированных пользователей к сетевым службам RF MAC.

Интерфейс BPI+ обеспечивает в общей среде передачи кабельной сети уровень защиты данных равный или лучше, чем уровень, который обеспечивают предназначенные для этого службы доступа к сети (аналоговые модемы или цифровые абонентские линии).

2 Ссылки

2.1 Нормативные

Указанные ниже рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все рекомендации и другие источники могут подвергаться пересмотру. Список действующих в настоящее время рекомендаций МСЭ-Т регулярно публикуется. Пользователям данной Рекомендации предлагается изучить возможность применения последнего издания рекомендаций и других источников, перечисленных ниже. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус рекомендации.

[SCTE22-2] ANSI/SCTE 22-2 2002, *DOCSIS 1.0 Часть 2: Спецификация интерфейса базовой защиты*, www.scte.org.

[SCTE23-3] ANSI/SCTE 23-3 2003, *DOCSIS 1.1 Часть 3: Интерфейс системы поддержки операций*, www.scte.org.

[SCTE79-2] ANSI/SCTE 79-2 2002, *DOCS 2.0 Интерфейс системы поддержки операций*, www.scte.org.

[J.112-B] Рекомендация МСЭ-Т J.112 Приложение B (2004), *Спецификации интерфейса службы передачи данных по кабелю: спецификация интерфейса радиочастот*.

[J.122] Рекомендация МСЭ-Т J.122 (2002), *Системы передачи второго поколения для интерактивных услуг кабельного телевидения – кабельные модемы IP*.

[FIPS-46-3] Федеральные публикации стандартов обработки информации 46-3, *Стандарт шифрования данных (DES)*, октябрь 1999 г.

[FIPS-140-2] Федеральные публикации стандартов обработки информации 140-2, *Требования безопасности для криптографических модулей*, май 2001 г.

[FIPS-180-2] Федеральные публикации стандартов обработки информации 180-2, *Стандарт безопасности хэш (SHS),* август 2002 г.

[PKCS № 7] IETF RFC 2315 (1998), *PKCS № 7: Синтаксис криптографического сообщения, версия 1.5*.

[RFC2104] IETF RFC 2104 (1997), *HMAC: Ключевое хэширование для идентификации сообщения*.

[RFC3083] IETF RFC 3083 (2001), *Основа информационного управления интерфейсом базовой защиты для DOCSIS совместимых кабельных модемов и систем окончаний кабельных модемов*.

[RFC3280] IETF RFC 3280 (2002), *Сертификат инфраструктуры открытого ключа Интернет X.509 и характеристики списка аннулированных сертификатов (CRL).*

[RSA3] *PKCS № 1: Спецификации криптографии RSA. Версия 2.0*, октябрь 1998 г.

[X.509] Рекомендация МСЭ-Т X.509 (2000) | ISO/IEC 9594-8:2001, *Информационная технология – Взаимодействие открытых систем – Руководство: Основы сертификата атрибутов открытого ключа.*

2.2 Информативные

[SCTE22-1] ANSI/SCTE 22-1 2002, *DOCSIS 1.0 Часть 1: Интерфейс радиочастот,* www.scte.org.

[SCTE22-3] ANSI/SCTE 22-3 2002, *DOCSIS 1.1 Часть 3: Интерфейс системы поддержки операций*, www.scte.org.

[DOCSIS4] *Спецификации интерфейса службы передачи данных по кабелю. Спецификация интерфейса оборудования кабельного модема в помещении пользователя*, SP-CMCI-I09-030730.

[DOCSIS8] *Основы информационного управления кабельных модемов DOCSIS и систем окончаний кабельных модемов для базовой защиты плюс*, draft-ietf-ipcdn-bpiplus-mib-05.txt, 8 мая 2001 г.

[FIPS-74] Федеральные публикации стандартов обработки информации 74, Руководство по применению и использованию стандарта шифрования данных *NBS*, апрель 1981 г.

[FIPS-81] Федеральные публикации стандартов обработки информации 81, *Режимы работы DES, декабрь 1980 г.* (включает извещение об изменении, ноябрь 1981 г.).

[FIPS-186-2] Федеральные публикации стандартов обработки информации 186-2, *Стандарт цифровой подписи (DSS)*, январь 2000 г.

[RFC2868] IETF RFC 2868 (2000), Атрибуты протокола *RADIUS для поддержки протокола туннелирования*.

[RSA1] Лаборатории RSA, *PKCS № 1: Стандарт шифрования RSA, версия 1.5*, RSA Security, Inc., Bedford, MA, ноябрь 1993 г.

[RSA2] Лаборатории RSA, *Некоторые примеры стандартов PKCS*, RSA Data Security, Inc., Redwood City, CA, ноябрь 1993 г.

3 Термины и определения

В данной Рекомендации определены следующие термины:

3.1 DOCSIS: Термин для системы или устройства, совместимого с любой системой или устройством лабораторий кабельного телевидения. Серия спецификаций ("CableLabs") расположена на сайте: http://www.cablemodem.com/specifications/.

3.2 DOCSIS 1.0: Система или устройство, совместимые со следующими спецификациями интерфейсов службы передачи данных по кабелю: [SCTE22-1], [SCTE22-2], [SCTE22-3], [DOCSIS4].

3.3 DOCSIS 1.1: Система или устройство, совместимые со следующими спецификациями интерфейсов службы передачи данных по кабелю: [J.112-B], [SCTE23-3], [DOCSIS4], а также с данной Рекомендацией.

3.4 DOCSIS 2.0: Система или устройство, совместимые со следующими спецификациями интерфейсов службы передачи данных по кабелю: [J.122], [SCTE79-2], [DOCSIS4], а также с данной Рекомендацией.

4 Сокращения

В данной Рекомендации использованы следующие сокращения:

BPI+	Управление ключом базовой защиты
CBC	Связанный блок шифрования
CM	Кабельный модем
CMTS	Система окончания кабельного модема
DES	Стандарт шифрования данных США
HMAC	Ключевое хэширование для идентификации сообщения
QoS	Качество обслуживания
RSA	Лаборатории RSA
SA	Ассоциация безопасности
SAID	Идентификатор ассоциации безопасности
SID	Идентификатор услуги
TEK	Ключ шифрования трафика

5 Основы и обзор базовой защиты плюс

Операторы кабельной сети заинтересованы в развертывании высокоскоростных пакетных систем передачи кабельного телевидения, которые способны поддерживать широкий спектр услуг. Рассматриваемые операторами кабельной сети услуги включают высокоскоростной доступ к Интернет, услугу пакетной телефонии, услугу видеоконференции, услугу ретрансляции кадров, эквивалентных потоку T1, и многое другое.

Предлагаемая услуга должна допускать прозрачную двустороннюю передачу трафика по протоколу Интернет – между окончанием кабельной системы и местоположением пользователей – по полностью коаксиальным или гибридным коаксиально/волоконным (HFC) сетям кабельного телевидения. В упрощенной форме это показано на рисунке 5-1.

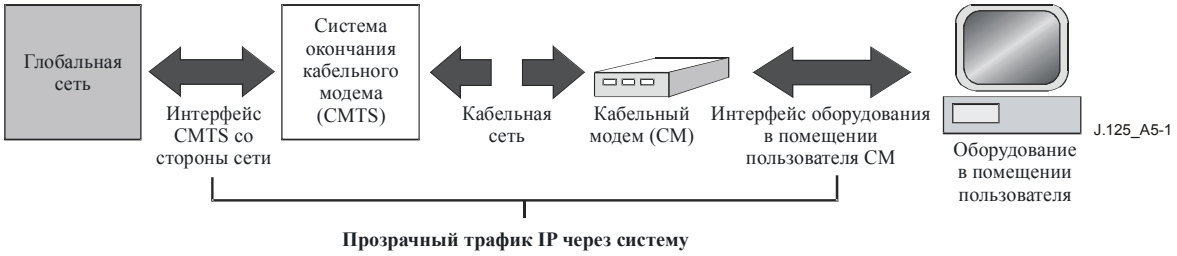


Рисунок 5-1/J.125 – Прозрачный трафик IP по системе передачи данных по кабелю

Канал передачи по кабельной системе реализован – в окончании с помощью CMTS, а у каждого пользователя – с помощью CM. В окончании (или в концентраторе) интерфейс к системе передачи данных по кабелю называют интерфейсом системы окончания кабельного модема – сторона сети (CMTS-NSI). В расположении пользователя этот интерфейс называют интерфейсом кабельного модема к оборудованию в помещении пользователя (CMCI). Это позволяет кабельным операторам прозрачно передавать IP трафик между этими интерфейсами, включая (но не ограничиваясь этим) диаграммы, DHCP, ICMP и групповую адресацию IP (вещание и групповую передачу).

Базовая защита (BPI) и базовая защита плюс (BPI+) обеспечивают пользователям кабельных модемов защиту данных в кабельной сети. Это достигается шифрованием потока трафика между CM и CMTS. Базовая защита – это исходный вариант такой функциональной возможности, который подробно описан в [SCTE22-2]. Базовая защита плюс – это обновленный вариант такой функциональной возможности, который является предметом данной Рекомендации. См. Приложение C для более подробного обсуждения разницы между этими двумя вариантами.

Кроме того, BPI+ обеспечивает операторам кабельных сетей хорошую защиту от хищения услуг. Защищенные услуги передачи данных MAC DOCSIS подразделяют на три категории:

- наилучший уровень из возможных, высокую скорость, услуги данных по IP;
- услуги передачи данных с QoS (т. е. с постоянной скоростью); и
- услуги групповой передачи по IP.

При BPI+ система CMTS защищает от несанкционированного доступа к этим транспортным услугам передачи данных с помощью принудительного шифрования соответствующих потоков трафика в кабельной сети. BPI+ использует протокол управления ключом идентификации клиент/сервер, в котором система CMTS, сервер, управляет распределением и вводом ключей для клиентов CM.

5.1 Обзор архитектуры

Базовая защита плюс содержит два протокола компонентов:

- Протокол инкапсуляции для шифрования пакетных данных в кабельной сети. Этот протокол определяет:
  1) формат кадра для транспортировки пакетных данных кадрами MAC DOCSIS;
  2) набор поддерживаемых криптографических комплектов, т. е. расположенных парами шифрованных данных и алгоритмов идентификации; и
  3) правила применения этих алгоритмов к кадрам пакетных данных MAC DOCSIS.
- Протокол управления кодом (управление кодом базовой защиты, или "BPKM") обеспечивает защищенное распределение данных о вводе ключей от системы CMTS к модемам CM. С помощью этого протокола управления кодом CM и CMTS синхронизируют данные о ключах, а кроме того, CMTS использует этот протокол, чтобы осуществить условный доступ к услугам сети.

5.1.1 Шифрование пакетных данных

Услуги шифрования BPI+ определяют как набор расширенных услуг внутри подуровня DOCSIS MAC. Специфичную для BPI+ информацию заголовка пакета помещают в элемент расширенного заголовка базовой защиты внутри расширенного заголовка MAC.

К моменту выпуска этой Рекомендации, BPI+ поддерживал единственный алгоритм шифрования пакетных данных: связанный блок шифрования (CBC) по методу американского стандарта шифрования данных (DES) с алгоритмом [FIPS-46-2] [FIPS-81]. BPI+ не составляет пару DES CBC ни с одним алгоритмом идентификации пакетных данных. Дополнительные алгоритмы шифрования данных могут быть поддержаны в будущих расширениях спецификации протокола BPI+, и эти алгоритмы могут быть парными с алгоритмами идентификации данных.

Протокол BPI+ кодирует кадры пакетных данных MAC DOCSIS. Заголовок кадра DOCSIS MAC не кодируется. Сообщения управления MAC DOCSIS ДОЛЖНЫ быть отправлены в явной форме, чтобы облегчить регистрацию, присвоение рангов и нормальную работу подуровня DOCSIS MAC[1].

В Разделе 6 определен формат кадров DOCSIS MAC, в которых содержится полезная нагрузка зашифрованных пакетных данных.

[1] Заголовки DOCSIS MAC пакетов данных PDU и сообщения управления DOCSIS MAC не-BPI+ МОГУТ кодироваться, если соединяют часть фрагментов пакета, согласно [J.112-B] или [J.122].

5.1.2 Протокол управления кодом

Модемы CM используют протокол управления кодом базовой защиты, чтобы получить от CMTS материал распределения и ввода ключей авторизации и трафика, а также поддержать периодические обновления авторизации и кода. Чтобы обеспечить безопасность обмена кодами между CM и CMTS, протокол управления кодом использует цифровые сертификаты X.509 [ITU1], алгоритм шифрования открытым ключом [RSA3] и тройной двухключевой алгоритм DES.

Протокол управления кодом базовой защиты придерживается модели клиент/сервер, в которой CM – "клиент" BPKM – запрашивает материал распределения и ввода ключей, а CMTS – "сервер" BPKM – отвечает на эти запросы, обеспечивая частным клиентам CM получение только того материала распределения и ввода ключей, на которое они имеют право (авторизованы). Протокол BPKM использует управляющие сообщения MAC DOCSIS.

Интерфейс BPI+ использует криптографию с открытым ключом, чтобы установить общий секретный ключ (т. е. ключ авторизации) между CM и CMTS. Затем общий секретный ключ используют для защиты последующих обменов BPKM ключами шифрования трафика. Этот двухуровневый механизм распределения ключей позволяет обновлять ключи шифрования трафика без необходимости интенсивного вычисления заголовка при операциях с открытым ключом.

Система CMTS аутентифицирует клиента CM во время начального обмена при авторизации. Каждый CM имеет уникальный цифровой сертификат X.509, выпущенный производителем CM. Цифровой сертификат содержит открытый ключ CM наряду с другой идентифицирующей информацией: MAC адресом CM, идентификатором ID производителя и серийным номером. При запросе ключа авторизации, модем CM предоставляет CMTS свой цифровой ключ. Система CMTS проверяет цифровой сертификат и затем использует проверенный открытый ключ для шифрования ключа авторизации, который система CMTS отправляет обратно запрашиваемому модему CM.

Система CMTS объединяет подтвержденную идентичность кабельного модема с платежеспособностью пользователя и с данными услуг, к которым этот пользователь имеет право доступа. Таким образом, с помощью обмена ключом авторизации CMTS устанавливает подтвержденную идентичность клиента CM и услуги (т. е. специальные ключи шифрования трафика), к которым этот пользователь CM имеет право доступа.

Поскольку CMTS аутентифицирует модемы CM, эта система может защитить от попытки использовать *клонированный* модем, замаскированный под подлинный модем пользователя. Использование сертификатов X.509 предотвращает доступ в CMTS клонированных модемов по фальшивым мандатам.

Модемы CM ДОЛЖНЫ иметь встроенную на заводе персональную пару открытых ключей RSA или обеспечить внутренний алгоритм для динамической генерации такой пары ключей. Если CM полагается на внутренний алгоритм генерации своей пары ключей RSA, то CM ДОЛЖЕН генерировать пару ключей до первой инициализации базовой защиты, описанной в 5.2.1. Модемы CM со встроенной на заводе парой ключей RSA ДОЛЖНЫ также иметь встроенные на заводе сертификаты X.509. Кабельные модемы, которые полагаются на внутренний алгоритм генерации своей пары ключей RSA, ДОЛЖНЫ поддерживать механизм инсталлирования выпущенного производителем сертификата X.509, за которым следует генерация ключа.

Протокол BPKM подробно определен в Разделе 7.

5.1.3 Ассоциации безопасности BPI+

Ассоциация безопасности BPI+ (SA) – это набор информации о безопасности CMTS и одного или более общих клиентов CM, с помощью которого поддерживают защищенную связь в кабельной сети. BPI+ определяет три типа ассоциаций безопасности: первичную, статическую и динамическую. Первичная ассоциация безопасности связана с единственным CM и устанавливается, когда CM заканчивает регистрацию MAC DOCSIS. Статические ассоциации безопасности обеспечиваются внутри CMTS. Динамические ассоциации безопасности устанавливают и исключают "на лету", в ответ на запуск и завершение специальных потоков трафика (в нисходящем направлении). Статические и динамические SA могут разделяться многими CM.

Общая информация ассоциации безопасности включает ключи шифрования трафика и векторы инициализации CBC. Чтобы поддерживать будущие расширения BPI+, альтернативное шифрование данных и алгоритмы идентификации данных, параметры ассоциации безопасности BPI+ включают криптографический комплект идентификаторов, указывающих конкретное разделение на пары шифрования пакетов данных и алгоритм идентификации пакетов данных, использованных ассоциацией безопасности. К моменту выпуска данной Рекомендации, 56-битовый DES и 40-битовый

DES были единственными поддерживаемыми алгоритмами шифрования пакетных данных, и еще не поддерживалась ни одна пара алгоритмов идентификации пакетных данных[2].

BPI+ идентифицирует ассоциации безопасности с помощью 14-ти битового идентификатора ассоциации безопасности (SAID).

Каждый CM (с включенной BPI+) устанавливает исключительную первичную ассоциацию безопасности со своим CMTS. Все трафики модемов CM в восходящем направлении ДОЛЖНЫ быть зашифрованы, согласно исключительной первичной ассоциации безопасности. Идентификатор SAID, соответствующий первичной SA модема CM, ДОЛЖЕН быть равен идентификатору ID услуги (SID) CM первичной DOCSIS 1.1 или DOCSIS 2.0 ([J.112-B] или [J.122]). С другой стороны, хотя обычно все однонаправленные трафики в нисходящем направлении, которые направляют в устройство (устройства) CPE вслед за CM, шифруют согласно исключительной первичной ассоциации безопасности CM, отобранные в нисходящем направлении однонаправленные потоки трафика могут быть зашифрованы, согласно статическим или динамическим SA. То есть, в нисходящем направлении трафик МОЖЕТ быть зашифрован, согласно любому из трех типов SA. Однако в нисходящем направлении групповая передача пакетных данных IP обычно характерна для многих CM, и поэтому более вероятно шифрование, согласно статической или динамической SA, которые могут быть доступны многим CM, в противоположность первичной SA, которая ограничена единственным CM.

Совместимый CM ДОЛЖЕН поддерживать одну первичную SA, одну или более динамических SA, и одну или более статических SA. Совместимая система CMTS ДОЛЖНА поддерживать одну первичную SA и одну или более динамических SA, и МОЖЕТ поддерживать одну или более статических SA. Спецификация BPI+ не определяет число статических и динамических SA, которые требуются для этих устройств.

Используя протокол BPKM, CM запрашивает у CMTS материал распределения и ввода ключей SA. Система CMTS гарантирует, что каждый клиент CM, который имеет на это право, будет иметь доступ к ассоциациям безопасности.

Материал распределения и ввода ключа SA (т. е. ключ DES и вектор инициализации CBC) имеет ограниченный срок жизни. Когда система CMTS поставляет модему CM материал распределения и ввода ключей, эта система также обеспечивает CM информацией об остающемся сроке жизни. Система также отвечает на запросы CM о новом материале распределения и ввода ключей от CMTS, прежде чем в CMTS истечет срок действия ключа, которым пользуется CM. Протокол BPKM определяет, каким образом устройства CM и CMTS поддерживают синхронизацию кодирования.

5.1.4 Качество обслуживания SID QoS и SAID BPI+

Элемент расширенного заголовка BPI+ в кадрах DOCSIS MAC в нисходящем направлении содержит SAID BPI+, в котором шифруют кадры в нисходящем направлении. Если в нисходящем направлении кадр, кроме конкретного CM, имеет единственную адресацию пакета к устройству CPE, то этот кадр обычно шифруют, как первичную SA модема CM. В этом случае SAID должен быть равен целевому идентификатору первичного SID CM. Если в нисходящем направлении кадр является многоадресным пакетом, предназначенным для приема многими CM, то элемент расширенного заголовка должен содержать статический или динамический идентификатор SAID, помещенный в многоадресную группу. Идентификатор SAID (первичный, статический или динамический), в сочетании с другими полями элементов расширенного заголовка в нисходящем направлении, идентифицирует для принимающего модема конкретный набор материала распределения и ввода ключей, который требуется для расшифровки кадров DOCSIS MAC, зашифрованных в поле пакетных данных.

Поскольку весь трафик модемов CM в восходящем направлении шифруют, согласно с его единственной первичной SA, кадрам DOCSIS MAC в восходящем направлении, в отличие от кадров DOCSIS MAC нисходящего направления, не требуется содержать SAID BPI+ в их расширенных заголовках. Вместо этого, элемент EH базовой защиты МОЖЕТ содержать любой действующий идентификатор SID QoS, присвоенный CM.

Элемент расширенного заголовка базовой защиты служит кадрам для многих целей передачи пакетных данных DOCSIS PDU MAC в восходящем направлении. В дополнение к идентификации конкретного набора материала распределения и ввода ключей, использованного для шифрования кадра пакетных данных, этот элемент также обеспечивает механизм предоставления по запросу последовательных полос пропускания и переноса данных управления фрагментацией. Последние две функции связаны с конкретным SID QoS. Для этой цели элементы расширенного заголовка базовой защиты в восходящем направлении содержат SID QoS чаще, чем BPI+ первичного SAID, который можно найти из SID QoS.

---

[2] BPI+ шифрует пакеты PDU CRC Ethernet/802.3. Хотя это и создает некоторую степень идентификации данных, криптографически такая операция не обеспечивает идентификацию данных.

5.2 Обзор работы

5.2.1 Инициализация кабельного модема

Источники [J.112-B] или [J.122] разделяют инициализацию кабельного модема на такую последовательность задач:

- просмотреть канал в нисходящем направлении и установить синхронизацию с CMTS;
- получить параметры передачи;
- выполнить ранжирование (разделение на ранги);
- установить соединение IP (DHCP);
- установить дату и время;
- передать рабочие параметры (загрузить файл параметров через TFTP);
- зарегистрировать в CMTS.

За регистрацией в CMTS следует установка базовой защиты.

Если CM предполагает запустить базовую защиту, то установка включения защиты (тип 29) в файле конфигурации стиля DOCSIS 1.1 или 2.0 ДОЛЖНА быть явно/неявно установлена на включение, независимо от присутствия установок конфигурации базовой защиты (тип 17). Другими словами, для запуска базовой защиты установки конфигурации базовой защиты не требуют представления в файле конфигурации. Эти дополнительные установки конфигурации определены в Приложении A.

По завершении регистрации в CMTS, система CMTS должна иметь один или более присвоенных идентификаторов ID статической услуги (SID) для регистрации CM, которые соответствуют предоставленному CM статическому классу услуги. Первый статический SID, присвоенный во время процесса регистрации, является первичным SID, и этот SID будет также служить модему CM первичным SAID BPI+. Если CM сконфигурирован для запуска базовой защиты, за регистрацией в CMTS сразу следует инициализация защитных функций базовой защиты CM.

Инициализацию базовой защиты начинают с отправки от CM к CMTS сообщения с информацией идентификации вместе с сертификатом CA производителя CM и запросом авторизации со следующей информацией:

- данные, идентифицирующие CM (т. е. MAC адрес);
- открытый ключ RSA модема CM;
- сертификат X.509, подтверждающий связь между данными идентификации CM и открытым ключом CM;
- список возможностей безопасности CM (т. е. конкретные пары шифрования и поддержка алгоритмов идентификации CM); и
- первичный идентификатор SAID модема CM (т. е. первичной SID).

Если CMTS определяет, что запрашиваемый CM авторизован при запросе авторизации первичным SAID, система CMTS отправляет ответ на авторизацию, содержащий ключ авторизации, из которого CM и CMTS находят ключи, необходимые для защиты CM от последующих запросов на ключи шифрования трафика, а также ответы CMTS на эти запросы. Система CMTS шифрует ключ авторизации, принимая открытый ключ кабельного модема.

Ответ авторизации также содержит список дескрипторов ассоциации безопасности, идентифицирующие первичные и статические SA, на которые запрашиваемый CM имеет право доступа. Каждый дескриптор SA состоит из набора параметров SA, включая идентификатор SAID этой SA, тип и криптографию. Список содержит, по крайней мере, один элемент: дескриптор, описывающий первичную ассоциацию безопасности CM. Дополнительные элементы являются необязательными и должны описывать любую статическую SA, к которой этот CM имеет доступ.

После успешного завершения идентификации и авторизации на CMTS, кабельный модем отправляет CMTS запросы на ключи, запрашивая ключи шифрования трафика, чтобы использовать их с каждым из этих идентификаторов SAID. Запросы CM на ключи трафика идентифицируют, используя алгоритм ключевого хэша (HMAC [RFC 2104]). Ключ идентификации сообщения находят по ключу авторизации, который получен во время предыдущего обмена авторизацией. Система CMTS

отправляет запрос на ключи, содержащие ключи шифрования трафика (TEK). TEK – это утроенный стандарт DES, зашифрованный ключом шифрования, полученным из ключа авторизации. Подобно ключам запросов, ключи ответов удостоверяются ключевым хэшем, а ключ идентификации сообщения находят из ключа авторизации.

Инициализация базовой защиты заканчивается, когда CMTS отправляет или получает от CM сообщения ответа на ключ, связанные со всеми идентификаторами SAID в сообщении ответа авторизации.

5.2.2 Механизм обновления ключа кабельного модема

Ключи шифрования трафика, которыми CMTS обеспечивает клиентов CM, имеют ограниченный срок жизни. CMTS, вместе со значением ключа, предоставляет сведения об оставшемся сроке жизни в ответе на ключ, который система отправляет клиентам CM. CMTS отслеживает, какие ключи являются текущими, сбрасывая ключи с истекшим сроком и генерируя новые ключи. Система несет ответственность за отдельные кабельные модемы, чтобы гарантировать, что ключи, которые используют модемы, совпадают с теми, которые использует CMTS. Кабельные модемы выполняют эту операцию, отслеживая, когда истекает предписанный срок конкретного идентификатора SAID ключа, и выдают запрос на новый ключ до истечения времени действия предыдущего.

Кроме того, кабельные модемы требуют периодической реавторизации (повторной авторизации) на CMTS. Как и в случае с ключами шифрования трафика, ключ авторизации имеет конечный срок жизни, который CMTS поставляет CM вместе со значением ключа. Каждый кабельный модем отвечает за реавторизации и доставку нового ключа авторизации (а также обновление списка дескрипторов SA), прежде чем CMTS аннулирует текущий ключ авторизации CM.

Инициализация базовой защиты и обновление ключа включают в протокол управления кодом базовой защиты, подробно рассмотренный в Разделе 7.

6 Форматы кадров DOCSIS MAC

При работе с включенным протоколом BPI+, каждый раз после окончания инициализации базовой защиты, система CMTS и CM ДОЛЖНЫ шифровать области данных PDU для всех из приведенных ниже двух типов кадров DOCSIS MAC, передаваемых по кабельной сети, и НЕ ДОЛЖНЫ передавать по кабельной сети никакие данные без их шифрования до тех пор, пока это не будет в явной форме разрешено спецификацией DOCSIS или явно обозначено оператором:

- кадры пакетов данных PDU MAC переменной длины;
- кадры фрагментации MAC.

В каждом из этих двух случаев элемент расширенного заголовка базовой защиты в заголовке DOCSIS MAC идентифицирует ассоциацию безопасности и сопровождает материал распределения и ввода ключей, использованный для шифрования данных PDU.

6.1 Формат PDU MAC пакетов данных переменной длины

На рисунке 6-1 показан формат кадра пакетов данных PDU DOCSIS переменной длины с элементом защиты расширенного заголовка (EH) и зашифрованной полезной нагрузкой пакетов PDU.

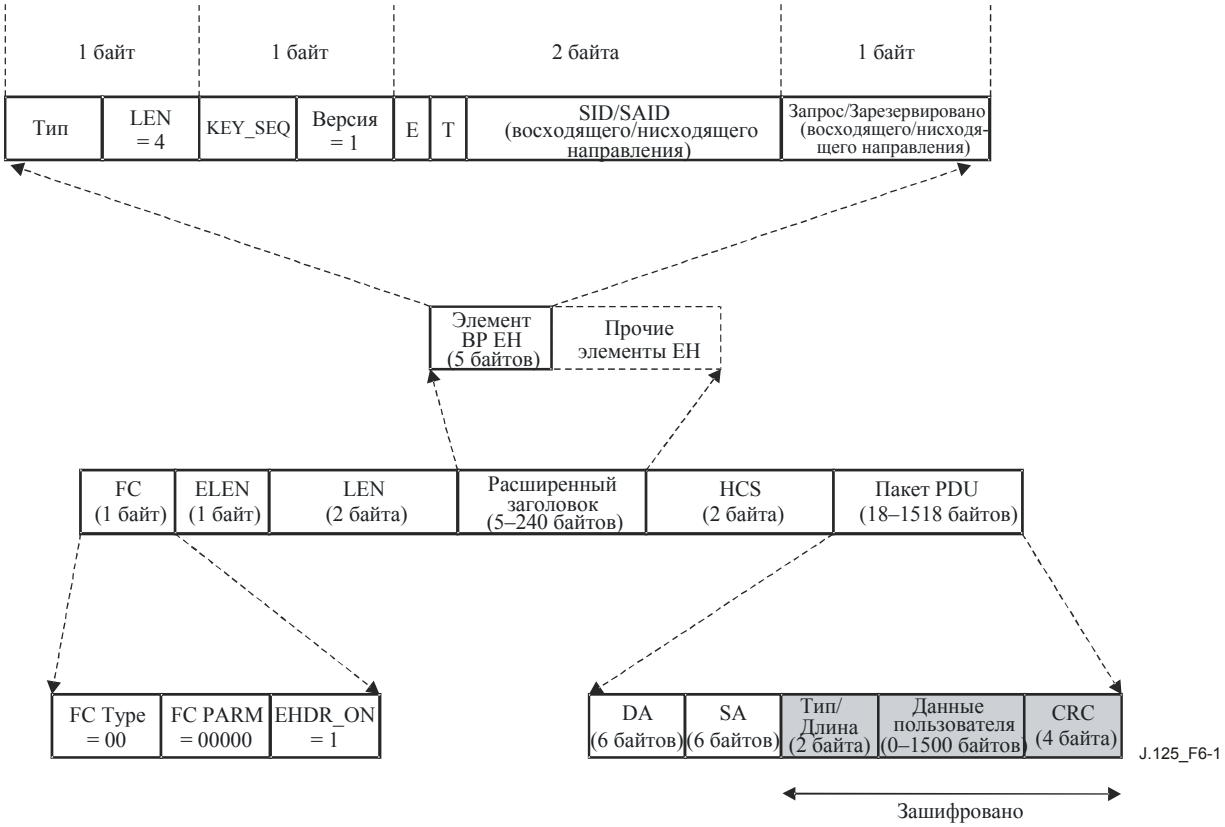


Рисунок 6-1/J.125 – Формат DOCSIS пакетов данных PDU переменной длины с элементом защиты EH

Первые 12 октетов из пакетов PDU, содержащих адрес назначения Ethernet/802.3 и источник адресов (DA/SA), не шифруют. Передаваемые адреса назначения кадров и источник адресации в явной форме обеспечивают поставщикам большую гибкость, позволяющую объединить шифрование/ дешифрование с помощью выполнения функций DOCSIS MAC. То есть поставщики имеют свободу выбора между фильтрацией DA/SA или SID. Контроль CRC пакетов PDU по Ethernet/802.3 шифруют.

Система CMTS включает элемент базовой защиты EH во всех нисходящих направлениях пакетов данных PDU, которые шифруют по методу базовой защиты плюс. Аналогично, модем CM включает элемент базовой защиты EH во всех восходящих направлениях пакетов данных PDU, которые шифруют по методу базовой защиты плюс. Если многочисленные элементы расширенного заголовка представлены в заголовке DOCSIS MAC, элемент расширенного заголовка базовой защиты ДОЛЖЕН быть первым.

Элемент защиты расширенного заголовка использует два типа значений EH: BPI_UP и BPI_DOWN – для восходящего и нисходящего направлений пакетов данных PDU, соответственно. Рекомендации [J.112-B] или [J.122] определяют специфику значений типов элементов EH. присвоенную BPI_UP и BPI_DOWN.

4 бита высокого разряда поля значения элемента расширенного заголовка BPI+ содержат номер последовательности ключей, KEY_SEQ. Напомним, что материал распределения и ввода ключей, связанный с BPI+ SAID, имеет ограниченный срок жизни. CMTS периодически обновляет материал распределения и ввода ключей SAID. Система CMTS управляет номером последовательности 4-х битовых ключей независимо для каждого SAID и распределяет номер последовательности ключей вместе с материалом распределения и ввода ключей SAID клиентам CM. Система CMTS увеличивает номер последовательности ключей при каждой новой генерации материала распределения и ввода ключей. Элемент защиты EH включает этот номер последовательности, вместе с SAID, чтобы идентифицировать особенность генерации этого идентификатора SAID материала распределения и ввода ключей, предназначенного для шифрования прикрепленных пакетов данных PDU. Из-за 4-х битового размера, номер последовательности переходит на новую строку 0, когда достигает 15.

Сравнивая полученные кадры номера последовательности ключей с тем, который считают "текущим" номером последовательности ключей, CM или CMTS могут легко распознать потерю синхронизации ключа в его ранге. Модем CM ДОЛЖЕН удерживать две самые последние генерации материала

распределения и ввода ключей для каждого BPI+ SAID. Удержание наготове этих двух последних генераций ключей необходимо для поддержания работы без перерывов во время смены идентификаторов SAID ключей.

Следующие 4 бита KEY_SEQ содержат номер версии протокола. Этот номер версии протокола устанавливают на 1 в заголовках PDU MAC пакетов данных переменной длины DOCSIS.

Следующие два байта содержат 2 бита статуса шифрования и 14 битов SID/SAID (SID – для кадров восходящего направления, SAID – для кадров нисходящего направления). Бит статуса шифрования ENABLE указывает, включено или отключено шифрование для данных PDU. Если бит ENABLE – это 0, то пакеты данных PDU не шифруют, и элемент EH базовой защиты ДОЛЖЕН игнорироваться (за исключением дополнительного запроса на транспортировку полосы пропускания – см. ниже). Бит TOGGLE ДОЛЖЕН соответствовать положению наименее значащего бита (LSB) номера последовательности ключей KEY_SEQ.

Протокол [J.112-B] или [J.122] DOCSIS MAC определяет запрос элемента EH на транспортировку полосы пропускания для передачи данных. Базовая защита определяет дополнительный механизм для запросов на транспортировку полосы пропускания: последний байт элемента EH базовой защиты в восходящем направлении (тип элемента EH = BPI_UP) несет дополнительный запрос на размещение полосы пропускания. Если имеется запрос на транспортировку, этот байт представляет номер запрошенного небольшого временного промежутка (слота). 14 битов SID в элементе EH базовой защиты в восходящем направлении идентифицируют служебный ID, который сопровождает запрос на полосу пропускания. Если в элементе EH базовой защиты отсутствует запрос, то байт запроса устанавливают на нуль. Запрос на транспортировку в элементе EH базовой защиты ДОЛЖЕН быть обработан, независимо от статуса бита ENABLE.

В нисходящем направлении передачи пакетов (тип элемента заголовка расширителя = BPI_DOWN), четвертый и последний байты зарезервированы и установлены на нуль.

Таблица 6-1/J.125 – Итоговая сводка содержания двух элементов EH базовой защиты

EH_TYPE	EH_LEN	EH_VALUE
BPI_UP См. [J.112-B] или [J.122]	4	KEY_SEQ (4 бита), Версия (4 бита), SID (2 байта), Запрос [piggyback] (1 байт) [CM → CMTS] Поле KEY_SEQ (4 бита): номер последовательности ключей Поле версии (4 бита) определено как: 0x1 Поле SID определено как: Bit[15]: ENABLE: 1..шифрование включено; 0..шифрование отключено Bit[14]: TOGGLE: 1..нечетный ключ; 0..четный ключ Bit[13:0]: служебный ID. Поле запроса содержи номер небольшого временного промежутка, запрошенного для полосы пропускания в восходящем направлении.

Таблица 6-1/J.125 – Итоговая сводка содержания двух элементов EH базовой защиты

EH_TYPE	EH_LEN	EH_VALUE
BPI_DOWN См. [J.112-B] или [J.122]	4	KEY_SEQ (4 бита), Версия (4 бита), SID (2 байта), Зарезервирован (1 байт) [CMTS → CM] Поле KEY_SEQ (4 бита): номер последовательности ключей Поле версии (4 бита) определено как: 0x1 Поле SAID определено как: Bit[15]: ENABLE: 1..шифрование включено; 0..шифрование отключено Bit[14]: TOGGLE: 1..нечетный ключ; 0..четный ключ Bit[13:0]: ID ассоциации безопасности. Зарезервированное поле установлено на 0.

В случае зашифрованных пакетов данных PDU, передаваемых в интервале соединения данных восходящего направления, идентификатор SID в элементе EH базовой защиты ДОЛЖЕН идентифицировать SID QoS. Идентификатор SID НЕ ДОЛЖЕН устанавливаться на служебный ID многоадресного запроса на соединение данных.

6.2 Формат кадра фрагментации MAC

Чтобы поддерживать фрагментацию в восходящем направлении кадры DOCSIS MAC, DOCSIS 1.1 или DOCSIS 2.0, изменяют элемент EH базовой защиты, чтобы переносить оба поля – шифрования и фрагментации [J.112-B] или [J.122]. Для функционирования в такой роли, элемент EH базовой защиты в восходящем направлении (тип элемента EH BPI_UP) расширяют на один байт, и последний байт служит как поле управления фрагментацией. На рисунке 6-2 показан формат кадра фрагментации MAC DOCSIS с зашифрованной полезной нагрузкой.

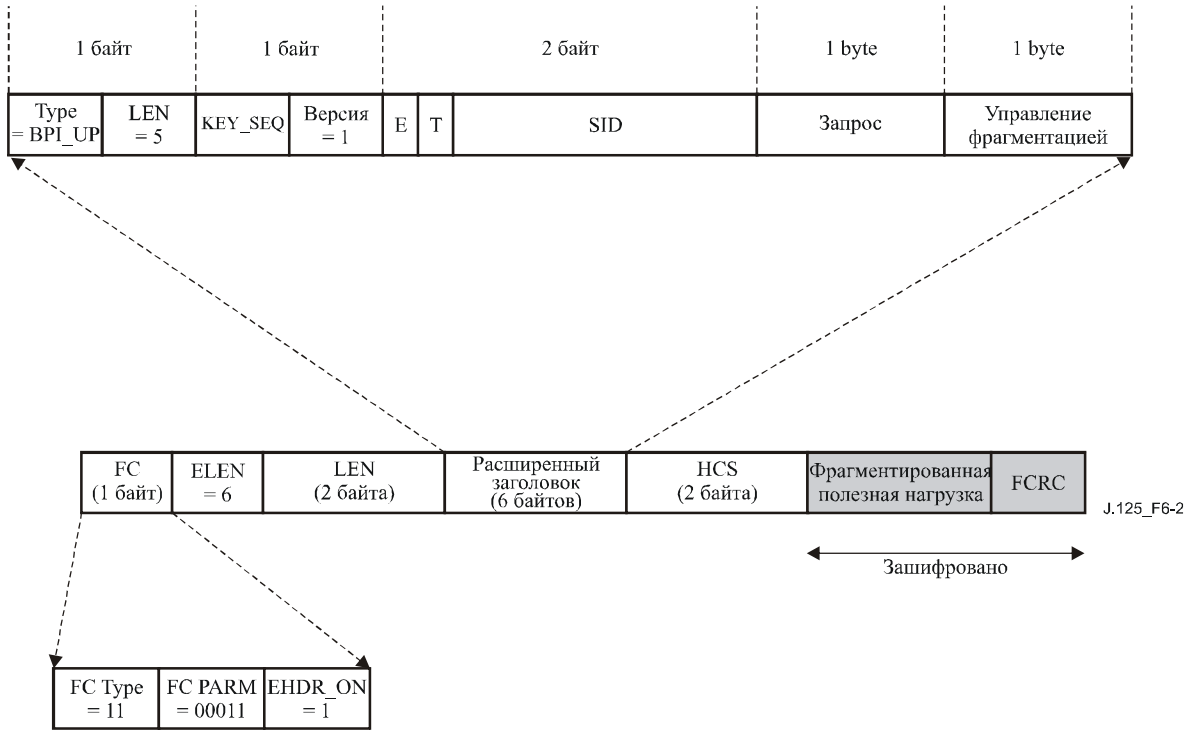


Рисунок 6-2/J.125 – Формат кадра фрагментации MAC DOCSIS с зашифрованной полезной нагрузкой

Типы FC = 11 и FC PARM = 00011 идентифицируют кадр MAC DOCSIS как кадр фрагментации. В отличие от кадров пакетов данных PDU MAC, кадры фрагментации MAC имеют фиксированный размер (шесть байтов) расширенного заголовка MAC, содержащего "растянутый" элемент EH базовой защиты.

За заголовком фрагментации MAC следует полезная нагрузка фрагмента и CRC фрагмента. При использовании шифрования базовой защиты, кадр фрагментации MAC, т. е. собственно полезную нагрузку фрагмента шифруют вместе с CRC фрагмента. Другими словами, в отличие от шифрования при базовой защите пакетов данных PDU, в полезной нагрузке перед началом шифрования отсутствует 12-ти байтовый сдвиг[3].

Поле LEN элемента EH базовой защиты в кадрах фрагментации MAC составляет чаще 5, чем 4 байта, учитывая дополнительный 1 байт поля управления фрагментацией. Поле KEY_SEQ, поле VERSION, флаги ENABLE и TOGGLE, а также поле SID – это то, что составляет кадр PDU MAC передачи пакетов данных в восходящем направлении.

Таблица 6-2/J.125 – Итоговая сводка содержания элемента EH базовой защиты кадра фрагментации MAC DOCSIS

EH_TYPE	EH_LEN	EH_VALUE
BPI_UP См. [J.112-B] или [J.122]	5	KEY_SEQ (4 бита), Версия (4 бита), SID (2 байта), запрос [piggyback] (1 байт), управление фрагментацией (1 байт) [CM → CMTS] Поле KEY_SEQ (4 бита): номер последовательности ключей Поле версии (4 бита) определено как: 0x1 Поле SID определено как: Bit[15]: ENABLE: 1..шифрование включено; 0..шифрование отключено Bit[14]: TOGGLE: 1..нечетный ключ; 0..четный ключ Bit[13:0]: служебный ID. Поле запроса содержит номер небольшого временного промежутка, запрошенного для полосы пропускания в восходящем направлении. Поле управления фрагментацией содержит специальную информацию об управлении фрагментацией; подробнее см. в [J.112-B] или [J.122].

Операция фрагментации отменяет BPI+ в том смысле, что модем CM ДОЛЖЕН первым определить, следует ли фрагментировать пакеты, основываясь на заданном размере (номере временного промежутка, который CMTS задал CM при расположении MAP полосы пропускания в восходящем направлении, [J.112-B] или [J.122]). Если пакеты не фрагментируют, шифрование BPI+ ДОЛЖНО производиться по фрагментам (на фрагментной основе), а не на основе PDU, как в остальных случаях. Каждый фрагмент должен иметь собственный заголовок фрагментации и шифроваться отдельно. Если пакет не фрагментируют, то он ДОЛЖЕН быть зашифрован одним блоком, с одним заголовком защиты.

6.3 Требования к применению элемента расширенного заголовка BP в заголовке MAC

Если BPI+ не включен в конкретный поток трафика нисходящего направления (т. е. одноадресный трафик CM или отдельная многоадресная группа IP), то элемент расширенного заголовка BP НЕ СЛЕДУЕТ использовать.

Если BPI+ не включен в одноадресный трафик CM, кадры, фрагментированные в восходящем направлении, ДОЛЖНЫ все же использовать элемент расширенного заголовка BP, но с

[3] Для не фрагментированных каров первые 12 байтов оставляют пустыми, чтобы перешифровать фильтрацию DA/SA. Для фрагментированных каров фильтрация DA/SA не может производиться раньше, чем будут реорганизованы пакеты. Поэтому нет смысла поддерживать шифрование 12-ти байтового сдвига в кадрах фрагментации MAC DOCSIS.

выключенным (0) битом шифрования ENABLE. Таким образом, расширенный заголовок BP можно все же использовать для запросов на транспортировку полосы пропускания, согласно правилам фрагментации, описанным в [J.112-B] или [J.122].

Для кадров MAC, состоящих только из заголовка MAC и опционально EHDR, базовая защита ДОЛЖНА быть отключена. Элемент базовой защиты EHDR МОЖЕТ быть представлен в этих кадрах, но бит ENABLE ДОЛЖЕН быть удален, чтобы отключить защиту.

7 Протокол управления ключом базовой защиты (BPKM)

7.1 Модели состояний

7.1.1 Введение

Протокол BPKM определен двумя различными, но взаимозависимыми моделями состояний: модель состояния авторизации (устройство состояния авторизации) и модель состояния ключа эксплуатационной службы (ключа шифрования трафика или устройства состояния TEK). Этот раздел определяет эти две модели состояний. Модели состояний введены только для целей объяснения и не накладывают ограничений на реальное использование.

Авторизация кабельного модема, управляемая машиной состояния авторизации, – это следующие процессы:

- CMTS подтверждает идентичность клиента CM;
- CMTS производит подтверждение CM ключом авторизации, из которых получают ключ шифрования ключей (KEK) и сообщение идентификации ключей;
- CMTS производит подтверждение идентичности (т. е. SAID) CM и свойств первичной и статической ассоциации безопасности CM и право получать для них информацию кодирования.

KEK является двухключевым тройным стандартом шифрования DES, который система CMTS использует для шифрования ключей шифрования трафика (TEK), которые отправляют модему. Ключи шифрования трафика используют для шифрования трафика пользовательских данных. Модем CM и система CMTS используют сообщения ключей идентификации для подтверждения (с помощью сжатого кодированного сообщения) запросов на ключи и ответов на них.

После получения первоначальной авторизации, кабельный модем периодически ищет в системе CMTS реавторизацию (повторную авторизацию). Реавторизацией также управляет машина состояния авторизации CM. Модем CM ДОЛЖЕН поддерживать свой статус авторизации в CMTS, чтобы быть в состоянии обновлять устаревшие ключи шифрования трафика. Машины состояния TEK управляют обновлением ключей шифрования трафика.

Кабельный модем начинает авторизацию отправкой своей системе CMTS информационного сообщения идентификации. Информационное сообщение идентификации содержит сертификат X.509 производителя кабельного модема. Информационное сообщение идентификации – это строго информативное сообщение, т. е. CMTS может его игнорировать, однако оно должно обеспечить для CMTS механизм возможности изучать сертификаты клиентов CM.

Кабельный модем отправляет CMTS сообщение запроса на авторизацию сразу после отправки информационного сообщения идентификации. Это – запрос на ключ авторизации, так же, как и для идентификации SAID каждой статической ассоциации безопасности, в которой имеет право участвовать модем CM. Запрос на авторизацию включает:

- серийный номер модема и ID производителя;
- MAC адрес кабельного модема;
- открытый ключ кабельного модема;
- выпущенный производителем сертификат X.509, связанный с открытый ключом кабельного модема и прочей информацией идентификации;
- описание криптографических алгоритмов, которые поддерживает запрашиваемый кабельный модем. Криптографические возможности CM представлены в CMTS в виде списка наборов криптографических идентификаторов, каждый из которых указывает на конкретную пару

шифрования пакетов данных и алгоритм пакетов данных идентификации, которые поддерживает этот CM;

- первичный SAID кабельного модема, *который равен первичному SID CM* (первичный идентификатор SID – это первый статический SID, который система CMTS присваивает CM во время регистрации RF MAC).

При ответе на сообщение запроса на авторизацию, когда CMTS проверяет запрос идентичности CM и определяет алгоритм шифрования и поддержку протокола, который их связывает, система CMTS ДОЛЖНА активировать ключ авторизации для CM, зашифровать его открытым ключом кабельного модема и отправить обратно модему CM в ответе на сообщение авторизации. Ответ авторизации включает:

- ключ авторизации, зашифрованный открытым ключом CM;
- 4-х битовый номер последовательности ключей, которые используют, чтобы различать последовательности генераций ключей авторизации;
- срок жизни ключа;
- идентичность (т. е. SAID) и свойства одной первичной и нулевой или более статических ассоциаций безопасности, для которых CM имеет право получать информацию кодирования.

Если CMTS поддерживает статические SA, в ответе модему на авторизации система CMTS ДОЛЖНА идентифицировать статические SA, связанные с CM, в дополнение к первичной SA, идентификатор которой SAID наилучшим образом соответствует запрашиваемому модемом CM идентификатору SID. Ответ авторизации НЕ ДОЛЖЕН идентифицировать никакие динамические SA.

В ответ на запрос на авторизацию, система CMTS должна определить, имеет ли право запрашиваемый кабельный модем, чья идентичность может быть проверена по цифровому сертификату X.509, на основные одноадресные услуги, и на какие статически поставляемые услуги (т. е. статические SAID) подписан пользователь кабельного модема.

ПРИМЕЧАНИЕ 1. – Защищенные услуги, предоставляемые CMTS клиенту CM, могут зависеть от конкретных криптографических наборов, которые совместно поддерживают CM и CMTS.

После авторизации, CM запускает самостоятельную машину состояния TEK для каждого из SAID, идентифицированного в ответном сообщении авторизации. Каждая машина состояния TEK, работающая в CM, отвечает за управление материалом распределения и ввода ключей, связанным с соответствующим SAID. Машины состояния TEK периодически отправляют CMTS сообщения запроса ключей, запрашивая обновление материала распределения и ввода ключей для своих соответствующих идентификаторов SAID. Запрос ключа включает:

- информацию идентификации единственности кабельного модема, состоящую из ID производителя, серийного номера, MAC адреса и открытого ключа RSA;
- идентификатор SAID, материал распределения и ввода ключей которого запрашивают;
- сжатое сообщение о ключах HMAC, подтверждающее запрос ключа.

Если CMTS подтверждает сжатое сообщение запроса ключа HMAC, система CMTS ДОЛЖНА ответить на сообщение запроса ключа сообщением ответа на запрос ключа, содержащее действующий материал распределения и ввода ключей CMTS для отдельного SAID, запрашивая идентичность CM и SAID. Этот материал распределения и ввода ключей включает:

- тройной по стандарту DES зашифрованный ключ шифрования трафика;
- вектор инициализации CBC;
- номер последовательности ключей;
- остающийся срок жизни ключа;
- сообщение HMAC о ключе, подтверждающее ответ на ключ.

Ключ шифрования трафика (TEK) в ответе на ключ – это тройное шифрование по стандарту DES (зашифровать–расшифровать–зашифровать, или режим EDE), которое использует двухключевой, тройной по стандарту DES ключ шифрования ключей (KEK), полученный из ключа авторизации.

ПРИМЕЧАНИЕ 2. – Каждый раз CMTS удерживает два действующих набора материала распределения и ввода ключей для каждого SAID. Сроки жизни двух генераций перекрываются таким образом, что каждая генерация остается действующий в течение половины жизни предшествующей, и не действующей в течение половины

жизни последующей генерации. Система CMTS включает в свои ответы на запросы ключа *оба* идентификатора SAID действующих генераций материала распределения и ввода ключей.

Ответ на запрос ключа обеспечивает запрашиваемому CM, в дополнение к TEK и CBC, вектор инициализации и остающийся срок жизни каждого из двух наборов материала распределения и ввода ключей. Принимающий CM использует эти остающиеся сроки жизни, чтобы оценить, когда CMTS сделает недействительным конкретный TEK, и, следовательно, когда наметит будущий запрос ключей, с тем чтобы CM запросил и получил новый материал распределения и ввода ключей до того, как CMTS аннулирует текущий материал распределения и ввода ключей CM.

Намеченный алгоритм запроса ключа машиной состояния TEK, вместе с управлением для обновления и использованием материала распределения и ввода ключей SAID (см. Раздел 9), гарантирует, что CM будет в состоянии непрерывно обмениваться с CMTS информацией о шифровании трафика.

Модем CM ДОЛЖЕН периодически обновлять свой ключ авторизации, повторно отправляя CMTS запрос на авторизацию. Реавторизация идентична авторизации, за исключением того, что CM не отправляет сообщений с информацией об идентификации во время циклов реавторизации. Описание машины состояния авторизации (см. 7.1.2) ясно указывает, когда отправляют сообщения с информацией об идентификации.

Чтобы избежать перерывов работы во время реавторизации, последующие генерации авторизаций ключей CM имеют перекрывающиеся сроки жизни. Как CM, так и CMTS ДОЛЖНЫ быть в состоянии поддерживать одновременно до двух действующих авторизаций ключей во время периодов смены. Работа намеченного алгоритма запроса машины состояния авторизации совместно с управлением системой CMTS обновлением и использованием авторизации ключей клиента CM (см. Раздел 9), гарантирует, что CM в периоды реавторизации будет в состоянии обновлять информацию о ключах TEK без перерывов.

Машина состояния TEK остается действующей пока:

- CM авторизуется, чтобы работать в безопасном домене CMTS; т. е. CM имеет действующий ключ авторизации; *и*
- CM авторизуется, чтобы участвовать в конкретной ассоциации безопасности; т. е. CMTS продолжает поставлять обновленный материал распределения и ввода ключей во время циклов смены ключей.

Родительская (корневая) машина состояния авторизации останавливает *все* младшие машины состояния TEK, когда CM получает от CMTS отказ на авторизацию во время цикла реавторизации. Отдельные машины состояния TEK могут запускаться и останавливаться во время цикла реавторизации, если авторизацию статического SAID меняют между последовательными реавторизациями.

Связь между авторизацией и машинами состояния TEK происходит с помощью событий и обмена сообщениями протокола. Машина состояния авторизации вырабатывает события (т. е. события останова (Stop), авторизации (Authorization), предстоящей авторизации (Authorization Pending) и завершения авторизации (Authorization Complete)), которые выполняют младшие машины состояния TEK. Машины состояния TEK не вырабатывают события на их родительской машине состояния авторизации. Машина состояния TEK влияет на машину состояния авторизации косвенно с помощью обмена сообщениями, которые CMTS отправляет в ответ на запросы модема: CMTS МОЖЕТ ответить отказом машине TEK на запрос ключей (т. е. сообщением недействительности авторизации), который будет направлен машиной состояния авторизации.

7.1.1.1 Предварительный комментарий к динамическим ассоциациям безопасности и отображении динамической SA

Раздел 5 посвящен динамическим SA и напоминает, каким образом CMTS может установить или исключить динамическую SA в ответ на создание или завершение потоков трафика в нисходящем направлении (например, отдельный трафик IP с многоадресной рассылкой). Для того, чтобы CM мог запустить машину состояния TEK и получить материал распределения и ввода ключей динамической ассоциации безопасности, модему CM требуется знать соответствующее значение SAID. Однако CMTS не свободно по отношению к клиентам CM с существующими динамическими SA. Вместо этого, CMTS отвечает на запросы CM об отображении идентификаторов потоков трафика (например, адресов IP при групповой рассылке) в динамические SAID.

Идентификатор BPI+ определяет обмен сообщениями, с помощью которых CM узнает об отображении потока трафика в нисходящем направлении в динамический SA (все трафики в восходящем направлении шифруют, согласно первичной SA модема CM). Машина состояния отображения SA определяет, как кабельные модемы управляют передачей этих запросов на сообщения отображения. В настоящее время только услуги управления многоадресной рассылкой IP DOCSIS реализуют этот механизм. В будущем могут быть использованы дополнительные услуги динамических SA BPI+.

Машина состояния авторизации управляет установлением и завершением действия машин состояния TEK, связанных с первичными и любыми статическими SA. Однако эта машина не управляет установлением и завершением действия машин состояния TEK, связанных с динамическими SA. Модемы CM ДОЛЖНЫ использовать необходимую логику для установления и завершения действия машин состояния TEK. Однако спецификация этого интерфейса не определяет, каким образом модемы CM могли бы управлять их динамическими SA машин состояния TEK.

Полное описание модели состояния отображении SA будет дано в Разделе 8.

7.1.1.2 Выбор возможностей защиты

В качестве части обмена при авторизации BPI+, модем CM обеспечивает CMTS списком всех криптографических наборов (пар данных шифрования и данных алгоритмов идентификации), которые поддерживает CM. Система CMTS выбирает из этого списка определенный криптографический набор для использования в запрашиваемых первичных SA модемов CM. Ответ авторизации, который CMTS отправляет обратно CM, включает дескриптор первичной SA, который, помимо прочего, идентифицирует криптографический набор, выбранный системой CMTS, чтобы использовать его для первичной SA модема CM. Система CMTS ДОЛЖНА отвергнуть запрос на авторизацию, если обнаружит, что ни один из предложенных криптографических наборов не является удовлетворительным.

Ответ на авторизацию также содержит необязательный список дескрипторов статических SA. Каждый дескриптор статической SA идентифицирует криптографический набор, используемый в SA. Выбор криптографического набора статических SA обычно делают независимо от запрашиваемых криптографических возможностях CM. Система CMTS МОЖЕТ включать в свой ответ на авторизацию дескрипторы статических SA, идентифицирующие криптографические наборы, которые не поддерживает запрашиваемый CM. Это – тот случай, когда CM НЕ ДОЛЖЕН запускать машины состояния TEK для статических SA, чьи криптографические наборы не поддерживает модем CM.

Приведенная выше структура выбора была включена в BPI+, чтобы поддерживать будущие расширения к оборудованию DOCSIS и протоколу BPI+. К моменту выпуска данной Рекомендации единственными алгоритмами шифрования пакетный данных, которые поддерживаются, являются 56-битовый DES и 40-битовый DES, и пока не существует никаких пар алгоритмов идентификации пакетных данных.

7.1.2 Машина состояния авторизации

Машина состояния авторизации состоит из шести состояний и восьми различных событий (включая получение сообщений), которые могут запускать переходы состояний. Конечная машина состояния авторизации (FSM) представлена ниже в графической форме как модель состояния потока (рисунок 7-1), а в форме таблицы – как матрица переходов состояний (таблица 7-1).

Диаграмма состояния потока показывает передаваемые сообщения протоколов и внутренние события, создаваемые для каждой модели состояний переходов. Однако эта диаграмма не указывает на дополнительные внутренние действия такие, как очистку или запуск таймеров, которые сопровождают специальные состояния переходов. Сопровождающая переходы состояний матрица – это подробное описание специальных действий, которые сопровождают каждое переход состояния. Матрица переходов состояний ДОЛЖНА быть использована в качестве определенной спецификации действий протокола, связанной с каждым переходом состояния.

Следующие условные обозначения используют в диаграмме последовательности действий машины состояния авторизации, как показано на рисунке 7-1.

- овалы – это состояния;
- события отмечены *курсивом*;
- сообщения отмечены обычным шрифтом;

- Переходы состояний (т. е. линии между состояниями) обозначают, <что вызывает переход>/<сообщения и события, запущенные переходом>. Так "*timeout*/Auth request" означает, что состояние получило событие "timeout" ("перерыв", "время ожидания") и отправляет сообщение запроса на авторизацию ("Auth request"). Если имеется много событий или сообщений перед косой чертой "/", разделенных запятой, то *любое* из них может быть причиной перехода. Если имеется много событий или сообщений, перечисленных после косой черты, то *все* специальные действия ДОЛЖНЫ сопровождать переход.

Матрица перехода состояний авторизации, представленная в таблице 7-1, перечисляет шесть состояний машины авторизации в самом верхнем ряду и восемь событий машины авторизации (включая приемы сообщений) – в крайнем левом столбце. Каждая клетка в матрице представляет специальную комбинацию состояний и событий со следующим состоянием (состояние, переходящее в), показанным в этой клетке. Например, клетка 4-B представляет прием сообщения ответа на авторизацию (Auth Reply) при состоянии ожидания авторизации (Auth Wait). В клетке 4-B содержится название следующего состояния, "авторизован". Таким образом, когда машина состояния авторизации СМ находится в состоянии ожидания авторизации и получено сообщение ответа на авторизацию, машина состояния авторизации переходит в состояние "авторизован". В связи с этим переходом состояния, ДОЛЖНЫ быть предприняты некоторые действия протокола, которые описаны в распечатке действий протокола под рубрикой 4-B в 7.1.2.5.

Затемненная клетка в матрице перехода состояния обозначает, что либо никакое специальное событие не может, либо не должно было бы произойти в этом состоянии, а если событие все же происходит, то машина состояния ДОЛЖНА его игнорировать. Например, если сообщение ответа на авторизацию получено в состоянии "авторизован", то это сообщение должно игнорироваться (клетк 4-C). Однако модем СМ МОЖЕТ, в ответ на ошибочное событие, зарегистрировать его появление, генерировать событие SNMP или предпринять некоторые другие действия, определенные поставщиком. Эти действия, однако, не определены в контексте машины состояния авторизации, которая просто игнорирует ошибочные события.

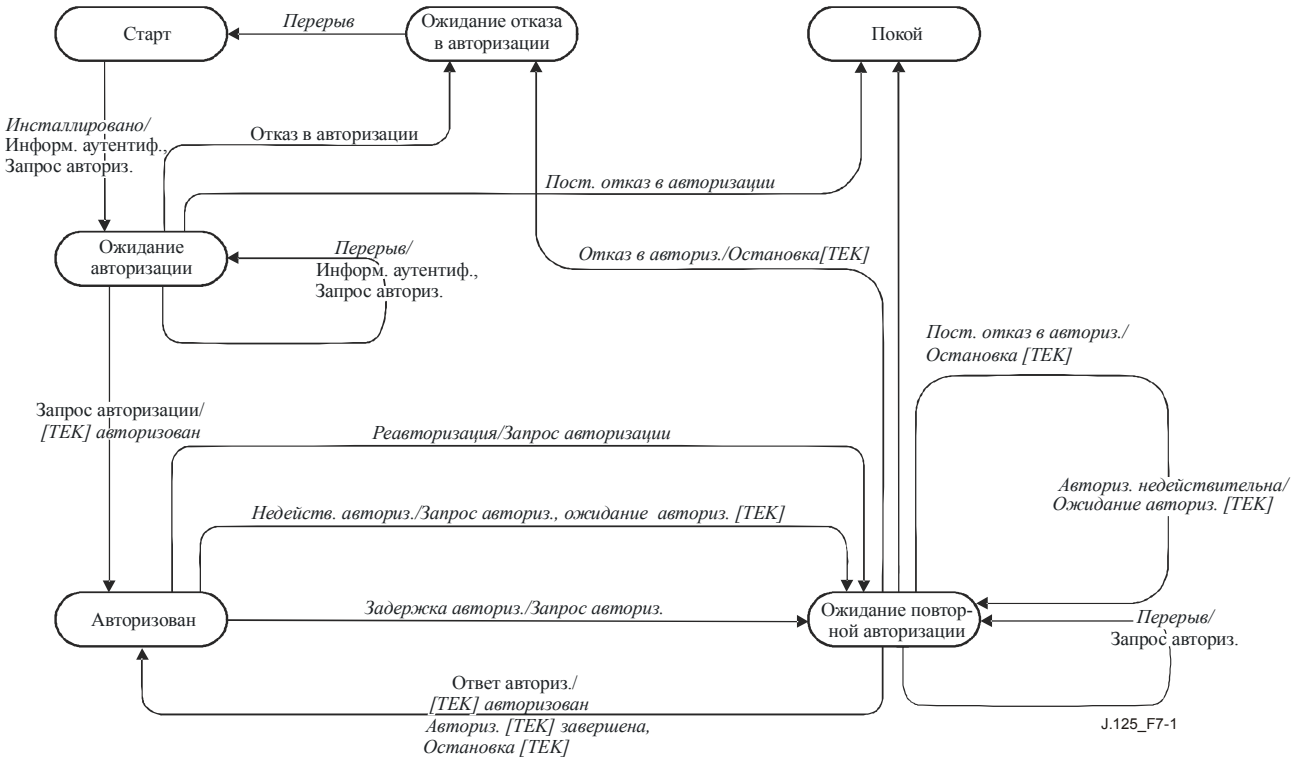


Рисунок 7-1/J.125 – Диаграмма последовательности действий машины состояния авторизации

Таблица 7-1/J.125 – Матрица переходов состояний авторизации FSM

Состояние / *событие или получ. сообщение*	(A) Старт	(B) Ожидание авторизизации	(C) Авторизован	(D) Ожидание реавторизации	(E) Ожидан. отказа на авториз.	(F) Покой
(1) *Предоставлено*	Ожидан. авториз.					
(2) *Отказ на авторизацию*		Ожидан. отказа на авториз.		Ожидан. отказа авториз.		
(3) *Долговрем. отказ на авторизацию*		Покой		Покой		
(4) *Ответ на авторизацию*		Авторизован		Авторизован		
(5) *Время ожидания*		Ожидан. авториз.		Ожидан. реавториз.	Старт	
(6) *Задержка ожидания*			Ожидан. реавториз.			
(7) *Авторизация недействительна*			Ожидан. реавториз.	Ожидан. реавториз.		
(8) *Реавторизация*			Ожидан. реавториз.			

7.1.2.1 Состояния

7.1.2.1.1 Старт (Start)

Это – первоначальное состояние FSM. В этом состоянии к FSM не приписаны и не используются никакие ресурсы. Например, все таймеры выключены, и не планируются никакая обработка.

7.1.2.1.2 Ожидание авторизации (Auth Wait)

Модем CM получил событие "Предоставлено", указывающее, что на CMTS закончена регистрация RF MAC. В ответ на получение этого события, CM посылает CMTS информацию идентификации и сообщение запроса на авторизацию и ждет ответ.

7.1.2.1.3 Авторизован (Authorized)

Модем CM получил сообщение ответа на авторизацию, которое содержит список действующих идентификаторов SAID для данного CM. С этого момента модем имеет действующий ключ авторизации и список SAID. Переход в это состояние запускает создание одной машины FSM TEK для каждого снабженного защитой идентификатора SAID модема CM.

7.1.2.1.4 Ожидание реавторизации (Reauth Wait)

CM ожидает выполнения повторного запроса на авторизацию. CM либо находился в конце времени ожидания текущей авторизации, либо получил указание (сообщение от CMTS о недействительности авторизации) о том, что его авторизация более недействительна. CM отправляет CMTS сообщение запроса на авторизацию и ждет ответа.

7.1.2.1.5 Ожидание отказа на авторизацию (Auth Reject Wait)

CM получил сообщение с отказом на авторизацию в ответ на последний запрос на авторизацию. Код ошибки отказа на авторизацию указал, что природа ошибки не долговременная. В ответ на получение сообщения отказа, CM устанавливает таймер и переходит в состояние ожидания отказа на авторизацию. CM остается в этом состоянии до времени истечения таймера.

7.1.2.1.6 Покой (Silent)

Модем CM получил сообщение с отказом на авторизацию в ответ на последний запрос на авторизацию. Код ошибки отказа на авторизацию указал, что природа ошибки не долговременная. Это запускает переход к состоянию покоя. В состоянии покоя CM НЕ ДОЛЖЕН пропускать трафик CPE, но ДОЛЖЕН быть в состоянии ответить на запросы управления SNMP, поступающие от

кабельной сети. Система CMTS МОЖЕТ предпочесть направить трафик данных какому-нибудь CM, который сможет расшифровать трафик в состоянии покоя, или CMTS МОЖЕТ заблокировать такой трафик.

7.1.2.2 Сообщения

Форматы сообщений подробно определены в пункте 7.2.

7.1.2.2.1 Запрос на авторизацию (Auth Request)

Запрос на авторизацию ключа и список авторизованных SAID. Отправляют в CMTS от CM.

7.1.2.2.2 Ответ на авторизацию (Auth Reply)

Получают ключ авторизации вместе со списком авторизованных статических идентификаторов SAID. Отправлено от CMTS к CM. Авторизацию ключа шифруют открытым ключом CM.

7.1.2.2.3 Отказ в авторизации (Auth Reject)

Попытка авторизации была отвергнута. Отправлено от CMTS к CM.

7.1.2.2.4 Авторизация не действительна (Auth Invalid)

Система CMTS может отправить сообщение о не действительности авторизации клиенту CM в виде:

- предоставленного добровольно указания; *или*
- ответа на сообщение, полученное от данного CM.

В любом случае сообщение о недействительности авторизации инструктирует принимающий CM о реавторизации на CMTS.

Система CMTS ДОЛЖНА ответить на запрос ключа сообщением о недействительности авторизации если:

1) CMTS не распознала, что CM авторизуется (т. е. не действует ключ авторизации, связанный с кабельным модемом); или
2) не удалась попытка проверки запроса ключа сжатым кодированным сообщением (атрибут сжатия – HMAC).

ПРИМЕЧАНИЕ. – Событие недействительности авторизации относится как к диаграмме состояния потока, так и к матрице переходов состояний. Это означает либо получение сообщения о недействительности авторизации, либо внутреннюю генерацию события.

7.1.2.2.5 Информация об идентификации (Authent Info)

Сообщение с информацией об идентификации содержит сертификат X.509 производителя кабельного модема, выпущенный DOCSIS. Сообщение Authent Info является строго информативным сообщением, которое CM отправляет CMTS. С его помощью CMTS МОЖЕТ динамически изучить сертификат производителя CM клиентов. Альтернативно, CMTS МОЖЕТ потребовать вне полосы список сертификатов производителей.

7.1.2.3 События

7.1.2.3.1 Предоставлено (Provisioned)

Машина состояния авторизации генерирует это событие после состояния старта, если RF MAC уже закончил инициализацию, т. е. регистрацию CMTS. Если RF MAC не закончил инициализацию, CM отправляет событие Provisioned машине авторизации FSM после завершения регистрации CMTS. Событие Provisioned побуждает CM начать процесс получение ключа авторизации и ключей TEK.

7.1.2.3.2 Время ожидания (Timeout)

Повторная передача или ожидание истечения времени таймера. Обычно вновь отправляют запрос.

7.1.2.3.3 Время задержки ожидания авторизации (Auth Grace Timeout)

Таймер задержки времени ожидания авторизации. Полагают, что время действия этого таймера (время задержки авторизации), сконфигурированного перед текущей авторизацией, истекло, что является сигналом модему CM для реавторизации, прежде чем истечет действительное время его авторизации. Время задержки авторизации определено при установке конфигурации в загруженном файле параметров TFTP.

7.1.2.3.4 Реавторизация (Reauth)

Можно заменить набор авторизованных статических идентификаторов SAID модема. Это событие генерируют в ответ на набор SNMP, [DOCSIS8], что означает запуск цикла реавторизации (повторной авторизации).

7.1.2.3.5 Авторизация не действительна (Auth Invalid)

Это событие может быть сгенерировано модемом внутри, когда происходит неудачная попытка подтверждения ответа на запрос ключа, отказ в ключе, или сообщение о недействительности ключа TEK или внешнее сообщение о недействительности авторизации, отправленное из CMTS модему CM. Система CMTS отвечает на запрос ключа о недействительности авторизации, если проверка сообщения кода идентификации закончилась неудачей. Оба случая указывают, что CMTS и CM потеряли синхронизацию авторизации ключа.

Система CMTS МОЖЕТ также отправить CM предоставленное добровольно сообщение о недействительности авторизации, форсируя событие недействительности авторизации.

7.1.2.3.6 Долговременный отказ на авторизацию (Perm Auth Reject)

Система CMTS ДОЛЖНА отправить сообщение отказа на авторизацию с кодом ошибки 6 (Долговременный отказ на авторизацию) в ответ на сообщение запроса на авторизацию при любом из следующих условий:

- действие сертификата CM несостоятельно, согласно 12.4.2 (это означает, что сертификат CM отмечен как недействительный);
- несовместимые возможности защиты.

Связанный с BPI+ документ OSS [DOCSIS8] обеспечивает описание конкретных объектов MIB CMTS, управляющих действиями, которые предпринимает CMTS в случае, если имеет место любое из вышеуказанных условий.

Когда CM получает отказ на авторизацию, указывающий на долговременные условия неудачи, машина состояния авторизации переходит в состояние покоя (Silent). Модемы CM ДОЛЖНЫ выдать событие DOCSIS после вступления в состояние покоя.

7.1.2.3.7 Отказ на авторизацию (Auth Reject)

Модем CM получает отказ на авторизацию в ответ на запрос на авторизацию. Код ошибки в отказе на авторизацию не указывает, что неудача произошла из-за условия долговременной ошибки. В результате машина состояния авторизации CM должна установить таймер ожидания и переход в состояние ожидания отказа на авторизацию. Модем CM остается в этом состоянии до тех пор, пока не истечет время таймера, после чего будет повторена попытка авторизации.

ПРИМЕЧАНИЕ. – Следующие события отправляются машиной состояния авторизации машине состояния TEK.

7.1.2.3.8 [TEK] Останов (Stop)

Отправляет FSM авторизации действующему (в состоянии non-START) FSM TEK, чтобы завершить FSM и удалить соответствующий материал распределения и ввода ключей SAID из таблицы ключей CM.

7.1.2.3.9 [TEK] Авторизован (Authorized)

Отправляет FSM авторизации не действующей (в состоянии non-START), но имеющей силу машине FSM TEK.

7.1.2.3.10 [TEK] Ожидаемая авторизация (Auth Pend)

Отправляет FSM авторизации специальной машине FSM TEK, чтобы указать, что FSM TEK находится в состоянии ожидания до тех пор, пока FSM авторизации не сможет завершить операцию реавторизации.

7.1.2.3.11 [TEK] Завершение авторизации (Auth Comp)

Отправляет FSM авторизации машине FSM TEK в состоянии ожидания оперативной реавторизации (Op Reauth Wait) или ожидания смены ключа реавторизации (Rekey Reauth Wait), чтобы очистить состояние ожидания, которое начала FSM TEK для события ожидаемой авторизации.

7.1.2.4 Параметры

Все конфигурации значений параметров определены в файле загрузки параметров TFTP (см. Приложение A: Расширения файла конфигурации TFTP).

7.1.2.4.1 Время ожидания авторизации (Auth Wait Timeout)

Период ожидания между отправками сообщений запроса на авторизацию из состояния ожидания авторизации. См. A.1.1.1.1.

7.1.2.4.2 Время ожидания реавторизации (Reauth Wait Timeout)

Период ожидания между отправками сообщений запроса на авторизацию из состояния ожидания реавторизации. См. A.1.1.1.2.

7.1.2.4.3 Время задержки ожидания авторизации (Auth Grace Timeout)

Отрезок времени до намеченного времени окончания функционирования авторизации, с которого CM начинает реавторизацию. См. A.1.1.1.3.

7.1.2.4.4 Время ожидания отказа авторизации (Auth Reject Wait Timeout)

Отрезок времени, в котором остается машина авторизации FSM модема CM в состоянии ожидания отказа на авторизацию перед переходом в состояние старт (Start). См. A.1.1.1.7.

7.1.2.5 Действия

Действия, предпринимаемые в связи с переходами состояний, перечислены ниже в списке <event/rcvd message> – <state> (<событие/получ. сообщение> – <состояние>):

1-A Start (*Provisioned*) → Auth Wait

- отправить сообщение с информацией об идентификации в CMTS;
- отправить сообщение запроса на авторизацию в CMTS;
- для повторного запроса на авторизацию установить таймер в положение Auth Wait Timeout.

2-B Auth Wait (*Auth Reject*) → Auth Reject Wait

- очистить таймер от повторного запроса на авторизацию;
- установить таймер в положение Auth Reject Wait Timeout.

2-D Reauth Wait (*Auth Reject*) → Auth Reject Wait

- очистить таймер от запроса на авторизацию;
- генерация события TEK FSM Stop для всех действующих машин состояния TEK;
- установить таймер в положение Auth Reject Wait Timeout.

3-B Auth Wait (*Perm Auth Reject*) → Silent

- очистить таймер от повторного запроса на авторизацию;
- отменить все переадресации трафика CPE.

3-D Reauth Wait (*Perm Auth Reject*) → Silent

- очистить таймер от повторного запроса на авторизацию;
- генерация события Stop FSM TEK для всех действующих машин состояния TEK;
- отменить все переадресации трафика CPE.

4-B Auth Wait (*Auth Reply*) → Authorized

- очистить таймер от повторного запроса на авторизацию;
- расшифровать и записать ключ авторизации, полученный в ответ на авторизацию;
- запустить машины FSM TEK для всех SAID, перечисленных в ответе на авторизацию (при условии, что CM поддерживает криптографический набор, который связан с SAID), и выдать событие "авторизовано" машинам FSM TEK для каждой из новых машин FSM TEK;
- установить "Время задержки ожидания авторизации" в положение выключить "Время задержки ожидания авторизации" (в секундах) до того, как истечет запланированное время поставки ключа авторизации.

4-D Reauth Wait (*Auth Reply*) → Authorized

- очистить таймер от повторного запроса на авторизацию;
- расшифровать и записать ключ авторизации, полученный в ответ на авторизацию;
- запустить машины FSM TEK для всех SAID, перечисленных в ответе на авторизацию (при условии, что CM поддерживает криптографический набор, который связан с SAID), и выдать событие "авторизован" машинам FSM TEK для каждой из новых машин FSM TEK;
- генерация события "Завершение авторизации" FSM TEK для любых текущих действующих машин FSM TEK, соответствующие идентификаторы SAID которых были перечислены в ответе на авторизацию;
- генерация события Stop TEK FSM для любых текущих действующих машин FSM TEK, соответствующие идентификаторы SAID которых не были перечислены в ответе на авторизацию;
- установить "Время задержки ожидания авторизации" в положение выключить "Время задержки ожидания авторизации" (в секундах) до того, как истечет запланированное время поставки ключа авторизации.

5-B Auth Wait (*Timeout*) → Auth Wait

- отправить сообщение с информацией об идентификации в CMTS;
- отправить сообщение с запросом на авторизацию в CMTS;
- установить повторно таймер запроса на авторизацию в положение Auth Wait Timeout

5-D Reauth Wait (*Timeout*) → Reauth Wait

- отправить сообщение запроса на авторизацию в CMTS;
- установить повторно таймер запроса на авторизацию в положение Reauthorize Wait Timeout.

5-E Auth Reject Wait (*Timeout*) → Start

- отсутствуют действия протокола, связанные с переходом состояния.

6-C Authorized (*Auth Grace Timeout*) → Reauth Wait

- отправить сообщение запроса на авторизацию в CMTS;
- установить повторно таймер запроса на авторизацию в положение Reauthorize Wait Timeout.

7-C Authorized (*Auth Invalid*) → Reauth Wait

- очистить таймер задержки ожидания авторизации;
- отправить сообщение запроса на авторизацию в CMTS;
- установить повторно таймер запроса на авторизацию в положение Reauthorize Wait Timeout;
- если событие недействительности авторизации связано к конкретной машиной FSM TEK, то при генерации события FSM TEK "Ожидаемая авторизация" машина состояния TEK отвечает на событие недействительностью авторизации (т. е. машина FSM TEK, которая либо генерировала событие, либо отправила сообщение запроса ключа в CMTS, отвечает на него сообщением недействительности авторизации).

7-D Reauth Wait (*Auth Invalid*) → Reauth Wait

- если событие недействительности авторизации связано к конкретной машиной TEK FSM, то при генерации события FSM TEK "Ожидаемая авторизация" машина состояния TEK отвечает на событие недействительностью авторизации (т. е. машина FSM TEK, которая либо генерировала событие, либо отправила сообщение запроса ключа в CMTS, отвечает на него сообщением недействительности авторизации).

8-C Authorized (*Reauth*) → Reauth Wait

- очистить таймер Задержки ожидания авторизации;
- отправить сообщение запроса на авторизацию в CMTS;
- установить повторно таймер запроса на авторизацию в положение Reauthorize Wait Timeout.

7.1.3 Машина состояния TEK

Машина состояния TEK состоит из шести состояний и девяти событий (включая прием сообщений), которые запускают переходы состояний. Подобно машине состояния авторизации, машина состояния TEK представлена как диаграммой состояния потока, так и матрицей переходов состояний. Как и в случае машины состояния авторизации, матрица переходов состояний ДОЛЖНА использоваться как окончательная спецификация действий протокола, связанных с каждым переходом состояний.

Затемненные состояния на рисунке 7-2 (Операционные, Ожидание смены ключа и Ожидание смены ключа реавторизации) имеют действующий материал распределения и ввода ключей и зашифрованный трафик, который может быть опущен.

Машина состояния авторизации запускает независимую машину состояния TEK для каждого из авторизованных SAID.

Как упоминалось ранее в 7.1.1, система CMTS поддерживает два действующих ключа TEK на один идентификатор SAID. Система CMTS включает в свой запрос ключа оба эти ключа TEK, вместе с остающимися их сроками жизни. Система CMTS шифрует трафик в нисходящем направлении двумя старыми ключами TEK и дешифрует трафик в восходящем направлении либо старым, либо новым ключом TEK, в зависимости от того, какой из этих ключей использует в это время CM. Модем CM шифрует трафик в восходящем направлении одним из новых ключей TEK и дешифрует трафик в нисходящем направлении либо старым, либо новым ключом TEK, в зависимости от того, какой из этих ключей использует в это время CMTS. См. Раздел 9 для подробностей о требованиях к использованию ключей в CM и в CMTS.

Во время работы машины состояния TEK, модем CM пытается сохранить копии ключей TEK SAID, синхронизированных с такими же ключами CMTS. Машина состояния TEK выдает запросы на ключи, чтобы обновлять копии материала распределения и ввода ключей SAID после запланированного истечения времени наиболее старого из двух ключей TEK и прежде, чем истечет время наиболее нового ключа TEK. Чтобы приспособиться к сдвигу времени CM/CMTS и другим задержкам системы обработки и передачи, модем CM планирует запрос на ключи с помощью регулируемого числа секунд (*m. e.* "Время задержки TEK" – "TEK Grace Time") прежде, чем истечет новое время действия ключа TEK, рассчитанное в CMTS. После приема ответа на запрос ключа, модем CM ДОЛЖЕН всегда обновлять свои записи параметров TEK, взятых из обоих ключей TEK, которые содержатся в сообщении ответа на запрос ключа. рисунок 9-2 иллюстрирует планирование модемом CM обновления ключа совместно с его управлением действующими ключами TEK SA на интерфейсе BPI+.

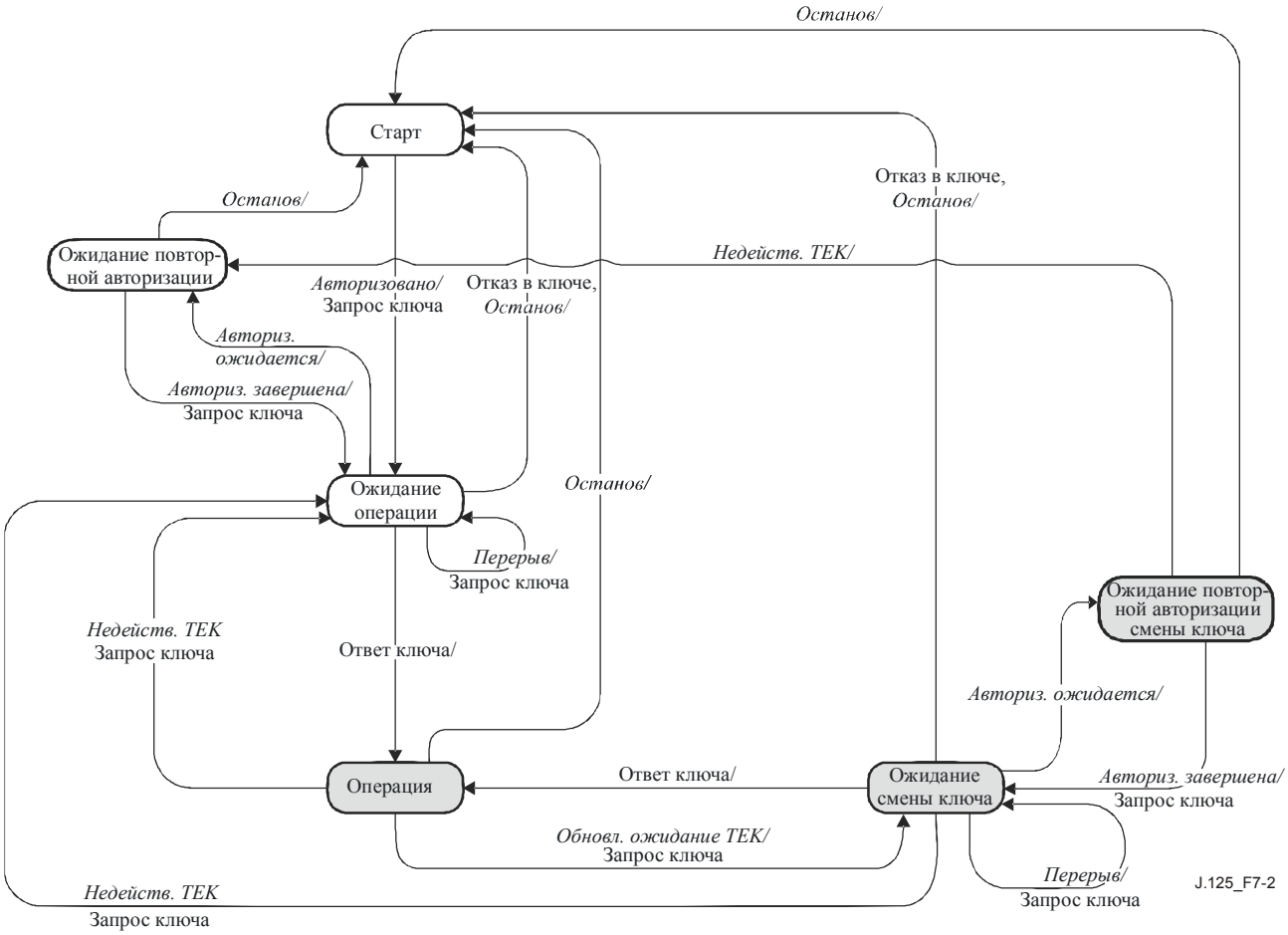


Рисунок 7-2/J.125 – Диаграмма последовательности действий машины состояния ТЕК

Таблица 7-2/J.125 – Матрица переходов состояний FSM ТЕК

Состояние / ***событие или получ. сообщение***	**(A) Старт**	**(B) Ожидание операции**	**(C) Ожидание операции реавториз.**	**(D) Оперативн. состояние**	**(E) Ожидание смены ключа**	**(F) Ожидание смены ключа для реавтор.**
(1) *Останов*		Старт	Старт	Старт	Старт	Старт
(2) *Авторизован*	Ожидан. операции					
(3) *Ожидаемая авторизация*		Ожидание операции реавториз			Ожидание смены ключа для реавтор.	
(4) *Завершение авторизации*			Ожидание операции			Ожидание смены ключа
(5) *Недейств.* ТЕК				Ожидание операции	Ожидание операции	Ожидание операции реавториз.
(6) *Время ожидания*		Ожидание операции			Ожидание смены ключа	
(7) *Обновл. время ожидания*				Ожидание смены ключа		
(8) *Ответ на запрос ключа*		Оперативн. состояние			Оперативн. состояние	
(9) *Отказ в ключе*		Старт			Старт	

7.1.3.1 Состояния

7.1.3.1.1 Старт (Start)

Это – первоначальное состояние FSM. В этом состоянии к FSM не приписаны и не используются никакие ресурсы. Например, все таймеры выключены, и не планируются никакая обработка.

7.1.3.1.2 Ожидание операции (Op Wait)

Машина состояния TEK отправляет первоначальный запрос (запрос ключа) для своего идентификатора SAID материала распределения и ввода ключей (ключ шифрования трафика и вектор инициализации CBC) и ждет ответа от CMTS.

7.1.3.1.3 Ожидание операции реавторизации (Op Reauth Wait)

Машина состояния TEK находится в состоянии ожидания, если она не имеет действующего материала распределения и ввода ключей, а в это время машина состояния авторизации находится в середине цикла реавторизации.

7.1.3.1.4 Оперативное состояние (Operational)

Модем CM имеет действующий материал распределения и ввода ключей для соответствующего идентификатора SAID.

7.1.3.1.5 Ожидание смены ключей (Rekey Wait)

Ключ обновления таймера TEK стал недействительным и модем CM запросил обновление ключа для SAID.

ПРИМЕЧАНИЕ. – Более новый из двух ключей TEK еще не утратил силу и еще может быть использован как для шифрования, так и для дешифрования трафика данных.

7.1.3.1.6 Ожидание смены ключей для реавторизации (Rekey Reauth Wait)

Состояние ожидания, в котором находится машина состояния TEK, если эта машина имеет действующий материал распределения и ввода ключей трафика и предстоит запрос на самый последний материал распределения и ввода ключей, а машина состояния авторизации инициировала цикл реавторизации.

7.1.3.2 Сообщения

Форматы сообщений подробно определены в 7.2.

7.1.3.2.1 Запрос ключа (Key Request)

Запрос ключа TEK для данного SAID. Модем CM отправляет в систему CMTS и подтверждает сжатым кодированным сообщением. Ключ сообщения идентификации находят из ключа авторизации.

7.1.3.2.2 Ответ на запрос ключа (Key Reply)

Ответ от CMTS, в котором содержатся два набора действующего материала распределения и ввода ключей трафика для SAID. Система CMTS отправляет модему CM. Включает ключи шифрования трафика SAID по тройному стандарту DES, зашифрованные ключом шифрования ключей, полученным из ключа авторизации. Сообщение ответа на запрос ключа подтверждают сжатым кодированным сообщением. Ключ идентификации находят из ключа авторизации.

7.1.3.2.3 Отказ в ключе (Key Reject)

Система CMTS ДОЛЖНА отправить сообщение об отказе в ключе модему CM в ответ на сообщение запроса ключа, чтобы указать, что ключ не будет отправлен, если идентификатор SAID в сообщении запроса ключа более не действует. Сообщение об отказе в ключе подтверждают сжатым кодированным сообщением. Ключ идентификации находят из ключа авторизации.

7.1.3.2.4 Идентификатор TEK не действителен (TEK Invalid)

Система CMTS ДОЛЖНА отправить CM сообщение о недействительности ключа TEK, если она определит, что CM шифрует пакеты данных PDU в восходящем направлении недействующим ключом TEK; т. е. номер последовательности ключей TEK SAID, содержащийся в полученном элементе пакета расширенного заголовка базовой защиты, находится вне известного диапазона CMTS для действующих номеров последовательности данного SAID.

7.1.3.3 События

7.1.3.3.1 Останов (Stop)

Отправляет машина авторизации FSM действующей (в состоянии non-START) машине FSM TEK, чтобы завершить работу FSM TEK и удалить соответствующий материал распределения и ввода ключей SAID из таблицы ключей CM. См. 7.1.2.3.8.

7.1.3.3.2 Авторизован (Authorized)

Отправляет машина авторизации FSM не действующей (в состоянии START) машине FSM TEK, чтобы уведомить FSM TEK об успешной авторизации. См. 7.1.2.3.9.

7.1.3.3.3 Ожидаемая авторизация (Auth Pend)

Отправляет машина авторизации FSM машине FSM TEK, чтобы перевести FSM TEK в состояние ожидания, пока FSM авторизации завершает реавторизацию. См. 7.1.2.3.10.

7.1.3.3.4 Завершение авторизации (Auth Comp)

Отправляет машина авторизации FSM машине FSM TEK в состоянии ожидания оперативной реавторизации или ожидания смены ключа реавторизации, чтобы очистить состояние ожидания, которое начала FSM TEK событием ожидаемой авторизации. См. 7.1.2.3.11.

7.1.3.3.5 Недействительный идентификатор TEK (TEK Invalid)

Это событие может быть вызвано либо логикой дешифрации пакетов данных CM, либо приемом от CMTS сообщения о не действительности TEK.

Логика дешифрации пакетов данных CM приводит к событию не действительности TEK, если будет распознана потеря синхронизации ключей TEK и шифрование CMTS; т. е. номер последовательности ключей TEK SAID, содержащийся в полученном элементе пакета расширенного заголовка базовой защиты в нисходящем направлении, находится вне известного диапазона CMTS для действующих номеров последовательности данного SAID.

Система CMTS отправляет CM сообщение о не действительности TEK, что вызывает в модеме событие не действительности TEK, если логика дешифрации CMTS распознает потерю синхронизации ключей TEK между CMTS и CM.

7.1.3.3.6 Время ожидания (Timeout)

Повтор таймера времени ожидания. Обычно вновь передают конкретный запрос.

7.1.3.3.7 Обновление времени ожидания TEK (TEK refresh timeout)

Идентификатор TEK обновляет таймер времени ожидания. Это событие таймера является сигналом машине состояния TEK для выпуска запроса на новый ключ, чтобы обновить материал распределения и ввода ключей. Обновленный таймер устанавливают, чтобы включить настраиваемую продолжительность времени (*TEK Grace Time*), прежде чем истечет время действия более нового идентификатора TEK, который использует CM. Настройку производят через CMTS, чтобы включить TEK после истечения срока действия более старого из двух идентификаторов TEK.

7.1.3.4 Параметры (Parameters)

Все значения конфигурации параметров определены в загружаемом файле параметров TFTP (см. Приложение A).

7.1.3.4.1 Оперативное время ожидания (Operational Wait Timeout)

Период времени ожидания между отправками сообщений запроса ключей из состояния Op Wait. См. A.1.1.1.4.

7.1.3.4.2 Время ожидания смены ключа (Rekey Wait Timeout)

Период времени ожидания между отправками сообщений запроса ключей из состояния Rekey Wait Timeout. См. A.1.1.1.5.

7.1.3.4.3 Время задержки ожидания (TEK Grace Time)

Временной интервал в секундах до расчетного окончания срока действия идентификатора TEK, с которого CM начинает смену ключа для нового TEK.

Время задержки ожидания определено в установке конфигурации загружаемого файла параметров TFTP. Это время одинаково для всех SAID. См. A.1.1.1.6.

7.1.3.5 Действия

1-B Op Wait (*Stop*) →Start

- очистить таймер повторного запроса ключа;
- завершить FSM TEK.

1-C Op Reauth Wait (*Stop*) → Start

- завершить TEK FSM.

1-D Operational (*Stop*) → Start

- очистить таймер обновления TEK. Таймер установлен на отключение за *"Tek Grace Time"* секунд прежде, чем истечет новое время действия ключа TEK;
- завершить FSM TEK;
- удалить материал распределения и ввода ключей SAID из таблицы ключей.

1-E Rekey Wait (*Stop*) → Start

- очистить таймер повторного запроса ключа;
- завершить FSM TEK;
- удалить материал распределения и ввода ключей SAID из таблицы ключей.

1-F Rekey Reauth Wait (*Stop*) → Start

- завершить FSM TEK;
- удалить материал распределения и ввода ключей SAID из таблицы ключей.

2-A Start (*Authorized*) → Op Wait

- отправить сообщение запроса ключа в CMTS;
- установить таймер повторного запроса ключа на оперативное время ожидания.

3-B Op Wait (*Auth Pend*) → Op Reauth Wait

- очистить таймер повторного запроса ключа.

3-E Rekey Wait (*Auth Pend*) → Rekey Reauth Wait

- очистить таймер повторного запроса ключа.

4-C Op Reauth Wait (*Auth Comp*) → Op Wait

- отправить сообщение запроса ключа в CMTS;
- установить таймер повторного запроса ключа на оперативное время ожидания.

4-F Rekey Reauth Wait (*Auth Comp*) → Rekey Wait

- отправить сообщение запроса ключа в CMTS;
- установить таймер повторного запроса ключа на время ожидания смены ключа.

5-D Operational (*TEK Invalid*) → Op Wait

- очистить таймер обновления TEK;
- отправить сообщение запроса ключа в CMTS;

- установить таймер повторного запроса ключа на оперативное время ожидания;
- удалить материал распределения и ввода ключей SAID из таблицы ключей.

5-E Rekey Wait (*TEK In Invalid*) → Op Wait

- очистить таймер повторного запроса ключа;
- отправить сообщение запроса ключа в CMTS;
- установить таймер повторного запроса ключа на оперативное время ожидания;
- удалить материал распределения и ввода ключей SAID из таблицы ключей.

5-F Rekey Reauth Wait (*TEK In Invalid*) → Op Reauth Wait

- удалить материал распределения и ввода ключей SAID из таблицы ключей.

6-B Op Wait (*Timeout*) → Op Wait

- отправить сообщение запроса ключа в CMTS;
- установить таймер повторного запроса ключа на оперативное время ожидания.

6-E Rekey Wait (*Timeout*) → Rekey Wait

- отправить сообщение запроса ключа в CMTS;
- установить таймер повторного запроса ключа на время ожидания смены ключа.

7-D Operational (*TEK Grace Timeout*) → Rekey Wait

- отправить сообщение запроса ключа в CMTS;
- установить таймер повторного запроса ключа на время ожидания смены ключа.

8-B Op Wait (Key Reply) → Operational

ПРИМЕЧАНИЕ 1. – Ответ на запрос ключа передает сообщение идентификации.

- очистить таймер повторного запроса ключа;
- процесс содержит сообщение ответа на запрос ключа и включает новый материал распределения и ввода ключей базу данных ключей;
- Установить таймер обновления TEK на отключение за "Tek Grace Time" секунд прежде, чем истечет новое время действия ключа TEK

8-E Rekey Wait (Key Reply) → Operational

ПРИМЕЧАНИЕ 2. – Ответ на запрос ключа передает сообщение идентификации.

- очистить таймер повторного запроса ключа;
- обработка содержания сообщения ответа на запрос ключа и включение нового материала распределения и ввода ключей в базу данных ключей;
- Установить таймер обновления TEK на отключение за "Tek Grace Time" секунд прежде, чем истечет новое время действия ключа TEK.

9-B Op Wait (Key Reject) → Start

ПРИМЕЧАНИЕ 3. – Отказ в ключе передает сообщение идентификации.

- очистить таймер повторного запроса ключа;
- завершение FSM TEK.

9-E Rekey Wait (Key Reject) → Start

- очистить таймер повторного запроса ключа;
- завершить FSM TEK;
- удалить материал распределения и ввода ключей SAID из таблицы ключей.

7.2 Форматы сообщений управления ключом[4]

Управления ключом базовой защиты использует два типа сообщений MAC: BPKM-REQ и BPKM-RSP. Документы [J.112-B] и [J.122] определяют особенности свойств этих типов.

Таблица 7-3/J.125 – Сообщения MAC управления ключом базовой защиты

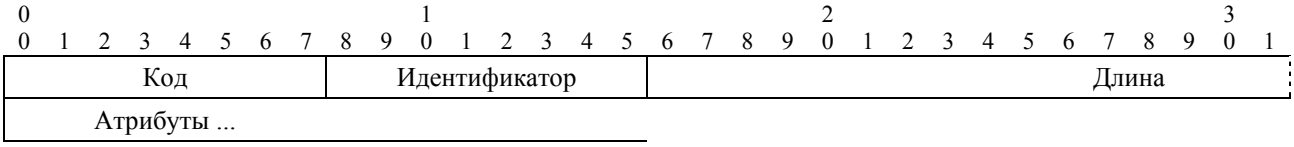
Значение типа	Имя сообщения	Описание сообщения
См. [J.112-B] или [J.122]	BPKM-REQ	Запрос на управление ключом защиты[CM → CMTS]
См. [J.112-B] или [J.122]	BPKM-RSP	Ответ на управление ключом защиты [CMTS → CM]

В то время как эти два типа сообщений управления MAC различаются между запросами BPKM (от CM к CMTS) и ответами (от CMTS к CM), более подробную информацию о содержании сообщения кодируют в самих сообщениях BPKM. Это позволяет поддерживать строгое разделение между функциями управления защиты и распределением полосы пропускания в восходящем направлении MAC RF, хронированием и синхронизацией (основные обязанности управления MAC RF).

7.2.1 Форматы пакетов

В поле полезной нагрузки сообщения управления MAC инкапсулируют точно одно сообщение BPKM.

Ниже приведен итоговый формат сообщения BPKM. Поля передают слева направо.



Код

Поле кода составляет один октет и идентифицирует тип пакета BPKM. Если пакет получен с недействительным полем кода, его СЛЕДУЕТ спокойно удалить.

Коды BPKM (десятичные) заданы следующим образом:

Таблица 7-4/J.125 – Коды сообщений управления ключом базовой защиты

Код	Тип сообщения BPKM	Наименование сообщения управления MAC
0-3	Зарезервировано	–
4	Auth Request	BPKM-REQ
5	Auth Reply	BPKM-RSP
6	Auth Reject	BPKM-RSP
7	Key Request	BPKM-REQ
8	Key Reply	BPKM-RSP
9	Key Reject	BPKM-RSP

[4] Форматы сообщений для протокола управления ключом базовой защиты моделируют после этих сообщений в протоколе удаленной идентификации набора в пользовательской службе (RADIUS), определенном в [RFC2868] и в протоколах ряда стандартов Интернет. Протокол BPKM, подобно RADIUS, подразумевает модель клиент/сервер. В отличие от RADIUS, протокол BPKM не может действовать в сети UDP/IP. Сообщения BPKM инкапсулируют в сообщения управления RF MAC.

Таблица 7-4/J.125 – Коды сообщений управления ключом базовой защиты

Код	Тип сообщения BPKM	Наименование сообщения управления MAC
10	Auth Invalid	BPKM-RSP
11	TEK Invalid	BPKM-RSP
12	Authent Info	BPKM-REQ
13	Map Request	BPKM-REQ
14	Map Reply	BPKM-RSP
15	Map Reject	BPKM-RSP
16-255	Зарезервировано	–

Идентификатор

Поле идентификатора состоит из одного октета. Модем CM использует идентификатор для согласовывания ответов CMTS с запросами CM.

Модем CM ДОЛЖЕН изменить (например, приращение при сбросе на 0 после достижения величины 255) поле идентификатора всякий раз, когда выпускает новое сообщение BPKM. "Новое" сообщение – это запрос на авторизацию, запрос ключа или запрос Map SA, который не передают повторно в ответ на событие "Время ожидания". Для повторной передачи поле идентификатора ДОЛЖНО оставаться неизменным.

Поле идентификатора в сообщениях с информацией об идентификации, которые являются информативными и не оказывают влияния на любые ответные сообщения, МОЖЕТ быть установлено на нуль.

Поле идентификатора в ответе на сообщение BPKM CMTS ДОЛЖНО соответствовать полю идентификатора сообщения запроса BPKM, на которое отвечает CMTS. Поле идентификатора в сообщениях о недействительности TEK, которые не отправляют в ответ на запросы о BPKM, ДОЛЖНО быть установлено на нуль. Поле идентификатора в сообщениях о предоставленной добровольно авторизации ДОЛЖНО быть установлено на нуль.

По получении сообщения ответа BPKM, CM связывает это сообщение с конкретной машиной состояния (машиной состояния авторизации в случае ответа на авторизацию, отказов в авторизации и недействительности авторизации; отдельной машиной состояния TEK в случае ответов на запросы ключа, отказов в ключе и недействительности TEK; отдельной машиной состояния отображения SA в случае ответов на отображение SA и отказов отображения SA).

Модем МОЖЕТ отслеживать самый последний идентификатор, намеченный запросом на авторизацию. Модем МОЖЕТ молчаливо аннулировать ответы на авторизацию и отказы в авторизации, если поля идентификатора не согласуются с такими же полями этих запросов.

Модем МОЖЕТ отслеживать самый последний идентификатор, с намеченным запросом ключа. Модем МОЖЕТ молчаливо аннулировать ответы на запросы ключа и отказы, если поля идентификатора не согласуются с такими же полями этих запросов.

Модем МОЖЕТ отслеживать самый последний идентификатор, с намеченным запросом на отображение SA. Модем МОЖЕТ молчаливо аннулировать ответы на запросы отображения SA и отказы, если поля идентификатора не согласуются с такими же полями этих запросов.

Длина

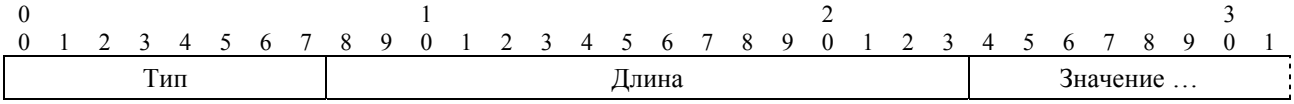
Поле длины составляет два октета. Оно указывает на длину полей атрибута в октетах. Поле длины не включает код, идентификатор и длину полей. Октеты вне диапазона поля длины ДОЛЖНЫ считаться заполнением и игнорироваться на приеме. Если пакет короче, чем поле длины, его СЛЕДУЕТ молчаливо аннулировать. Минимальная длина равна 0, а максимальная – равна 1490.

Атрибуты

Атрибуты BPKM отражают специфику идентификации, авторизации и управления ключом обмена данными между клиентом и сервером. Каждый тип пакета BPKM имеет собственный набор требуемых и необязательных атрибутов. За исключением ясно сформулированных случаев, отсутствуют требования на порядок атрибутов в сообщении BPKM.

Конец списка атрибутов обозначен длиной пакета BPKM.

Атрибуты типа/длины/значения (TLV) кодируют, как показано ниже. Поля передают слева направо.



Форматы пакетов для каждого из сообщений BPKM описаны ниже. Список описаний атрибутов BPKM содержатся в каждом типе сообщения BPKM. Собственно атрибуты описаны в 7.2.2. Неизвестные атрибуты ДОЛЖНЫ игнорироваться на приеме и пропускаться при просмотре для распознавания атрибутов.

Система CMTS ДОЛЖНА молчаливо отбрасывать все запросы, которые не содержат ВСЕ требуемые атрибуты. Модем CM ДОЛЖЕН молчаливо отбрасывать все ответы, которые не содержат ВСЕ требуемые атрибуты.

7.2.1.1 Запрос на авторизацию (Auth Request)

Код: 4

Атрибуты:

Таблица 7-5/J.125 – Атрибуты запроса на авторизацию

Атрибут	Содержание
CM-Identification	Содержит информацию, используемую для идентификации кабельного модема на CMTS
CM-Certificate	Содержит сертификат пользователя CM X.509
Security-Capabilities	Описывает запрашиваемые возможности защиты CM
SAID	Первичный SAID CM, равный первичному SID

Атрибут CM-Identification (идентификация модема CM) содержит набор данных, которые идентифицируют запрашиваемый кабельный модем для CMTS.

ПРИМЕЧАНИЕ. – При обработке система CMTS во всем подобна модему, используя только единственную позицию атрибута CM-Identification (например, MAC адрес модема). Несмотря на то, что в сообщение запроса на авторизацию можно включить специальную позицию, атрибут CM-Identification (идентификация клиента) обеспечивает поставщику большую гибкость при проектировании всей системы.

Атрибут CM-Certificate содержит сертификат X.509 CM, выпущенный производителем модема. Сертификат X.509 CM – это сертификат открытого ключа, который связывает информацию идентификации CM с открытым ключом RSA в поддающейся проверке форме. Сертификат X.509 является цифровой подписью производителя CM, и эта подпись может быть проверена системой CMTS, которой известен открытый ключ производителя. Открытый ключ производителя помещают в графу сертификата X.509 "certification authority" (CA), которую в свою очередь подписывает руководство более высокого уровня.

Атрибут Security-Capabilities (возможности защиты) является составным атрибутом, который описывает возможности защиты запрашиваемого кабельного модема. Атрибут включает алгоритм(ы) шифрования пакетов данных, который поддерживает CM, и поддерживаемый алгоритм(ы) идентификации пакетов данных (которые отсутствуют в настоящее время), а также версии поддерживаемых протоколов базовой защиты (из которых в настоящее время для BPI+ имеется только версия 1).

Атрибут SAID содержит идентификатор ассоциации безопасности базовой защиты, или SAID. В данном случае поставляемый SAID – это первичный идентификатор SAID BPI+ модема CM, который равен первичному идентификатору SID, присвоенному кабельному модему во время регистрации MAC RF.

7.2.1.2 Ответ на авторизацию (Auth Reply)

Система CMTS отправляет клиенту CM в ответ на запрос на авторизацию. Сообщение ответа на авторизацию содержит авторизацию ключа, срок жизни ключа, номер последовательности ключа и список SA-дескрипторов, идентифицирующих первичную и статическую ассоциации безопасности, на которые запрашиваемый кабельный модем имеет право доступа, а также их конкретные свойства (например, тип, криптографический набор). Авторизация ключа ДОЛЖНА быть зашифрована открытым ключом CM. Список SA-дескрипторов ДОЛЖЕН включать дескриптор для первичного идентификатора SAID BPI+, о котором сообщалось системе CMTS в соответствующем запросе на авторизацию. Список SA-дескрипторов МОЖЕТ включать дескрипторы статических идентификаторов SAID, на доступ к которым CM имеет право.

Поле кода: 5

Атрибуты:

Таблица 7-6/J.125 – Атрибуты ответа на авторизацию

Атрибут	Содержание
AUTH-Key	Авторизация ключа (AUTH), зашифрованная открытым ключом клиента CM
Key-Lifetime	Авторизация срока жизни ключа
Key-Sequence-Number	Авторизация номера последовательности ключа
SA-Descriptor (один или более)	Каждая составляющая атрибута SA-дескриптора определяет идентификатор SAID и дополнительные свойства SA.

7.2.1.3 Отказ в авторизации (Auth Reject)

Если CMTS отвергает запрос CM на авторизацию, CMTS отвечает на запрос авторизации модема CM сообщением отказа в авторизации.

Поле кода: 6

Атрибуты:

Таблица 7-7/J.125 – Атрибуты отказа в авторизации

Атрибут	Содержание
Error-code	Код ошибки, идентифицирующий причину отказа на запрос авторизации
Display-String (необязательный)	Строка отображения, сообщающая причину отказа на запрос авторизации

Атрибуты код ошибки и строка отображения описывают причину неудачи запроса CM на авторизацию.

7.2.1.4 Запрос ключа (Key Request)

Код: 7

Атрибуты:

Таблица 7-8/J.125 – Атрибуты запроса ключа

Атрибут	Содержание
CM-Identification	Содержит информацию, которую используют для идентификации кабельного модема в системе CMTS
Key-Sequence-Number	Номер последовательности ключа авторизации
SAID	ID ассоциации безопасности
HMAC-Digest	Сжатое сообщение с материалом распределения и ввода ключей SHA

Атрибут HMAC-Digest – это сжатое сообщение с материалом распределения и ввода ключей. Атрибут HMAC-Digest ДОЛЖЕН быть заключительным атрибутом в списке атрибутов запроса ключа. Сжатое сообщение помещают в заголовок пакета поверх всех атрибутов запроса ключа, иных чем HMAC-Digest, в таком порядке, в котором они появляются в пакете.

Включение сжатого сообщения с материалом распределения и ввода ключей позволяет системе CMTS идентифицировать сообщение запроса ключа. Ключ идентификации HMAC-Digest находят из ключа авторизации. Подробное описание см. в Разделе 10.

7.2.1.5 Ответ на запрос ключа (Key Reply)

Код: 8

Атрибуты:

Таблица 7-9/J.125 – Атрибуты ответа на запрос ключа

Атрибут	Содержание
Key-Sequence-Number	Номер последовательности ключа авторизации
SAID	ID ассоциации безопасности
TEK-Parameters	"Старая" генерация параметров ключа, существенная для SAID
TEK- Parameters	"Новая" генерация параметров ключа, существенная для SAID
HMAC-Digest	Сжатое сообщение с материалом распределения и ввода ключей SHA

Атрибут – это составной атрибут, содержащий все из материала распределения и ввода ключей, соответствующего конкретной генерации TEK SAID. Сюда включают TEK, остающийся срок жизни ключа TEK, номер его последовательности ключей и вектор инициализации CBC. Ключ TEK шифруют. Подробности см. в 7.2.2.13.

Все время CMTS содержит два набора действующих генераций материала распределения и ввода ключей на каждый SAID. (Набор материала распределения и ввода ключей включает TEK и соответствующий вектор инициализации CBC.) Один набор соответствует "старой" генерации материала распределения и ввода ключей, а второй – "новой" генерации. Новая генерация на единицу (по модулю 16) больше, чем номер предыдущей генерации. В пункте 9.1 определены требования к CMTS для поддержания и использования двух действующих генераций материала распределения и ввода ключей SAID.

Система CMTS отправляет клиенту CM обе генерации действующих материалов распределения и ввода ключей. Таким образом, сообщение ответа на запрос ключа содержит два атрибута TEK-Parameters, каждый из которых содержит материал распределения и ввода ключей для одного из двух действующих наборов материалов распределения и ввода ключей SAID.

Атрибут HMAC-Digest – это сжатое сообщение с материалом распределения и ввода ключей. Атрибут HMAC-Digest ДОЛЖЕН быть заключительным атрибутом в списке атрибутов ответа на

запрос ключа. Сжатое сообщение помещают поверх заголовка сообщения BPKM (начиная с поля кода BPKM) и всех атрибутов ответа на запрос ключа, иных чем HMAC-Digest, в таком порядке, в котором они появляются в пакете.

Включение сжатого сообщения с материалом распределения и ввода ключей позволяет принимающему клиенту идентифицировать сообщение ответа на запрос ключа и обеспечивает синхронизацию авторизации ключей CM и CMTS. Ключ идентификации HMAC-Digest находят из ключа авторизации. Подробное описание см. в Разделе 10.

7.2.1.6 Отказ в ключе (Key Reject)

Прием отказа в ключе указывает, что принимающий клиент CM более не имеет права на конкретный идентификатор SAID.

Код: 9

Атрибуты:

Таблица 7-10/J.125 – Атрибуты отказа в ключе

Атрибут	Содержание
Key-Sequence-Number	Номер последовательности ключа авторизации
SAID	ID ассоциации безопасности
Error-Code	Код ошибки, идентифицирующий причину отказа на запрос ключа
Display-String (необязательный)	Строка отображения, сообщающая причину отказа на запрос ключа
HMAC-Digest	Сжатое сообщение с материалом распределения и ввода ключей SHA

Атрибут HMAC-Digest – это сжатое сообщение с материалом распределения и ввода ключей. Атрибут HMAC-Digest ДОЛЖЕН быть заключительным атрибутом в списке атрибутов отказа в ключе. Сжатое сообщение помещают поверх заголовка сообщения BPKM (начиная с поля кода BPKM) и всех атрибутов отказа на запрос ключа, иных чем HMAC-Digest, в таком порядке, в котором они появляются в пакете.

Включение сжатого сообщения с материалом распределения и ввода ключей позволяет принимающему клиенту идентифицировать сообщение отказа на запрос ключа и обеспечивает синхронизацию авторизации ключей CM и CMTS. Ключ идентификации HMAC-Digest находят из ключа авторизации. Подробное описание см. в Разделе 10.

7.2.1.7 Недействительность авторизации (Authorization Invalid)

Система CMTS может отправить клиенту CM сообщение о недействительности авторизации в виде:

- добровольного указания; или
- ответа на сообщение, полученное от CM.

В любом случае, сообщение недействительности авторизации инструктирует принимающий CM вновь авторизоваться в системе CMTS.

Система CMTS отправляет сообщение недействительности авторизации в ответ на запрос ключа если:

1) CMTS не распознает, что CM авторизован (т. е. отсутствует действующий ключа авторизации, связанный с запросом кабельного модема); или
2) проверка на запрос ключа в сжатом сообщении с материалом распределения и ввода ключей (в атрибуте HMAC-Digest) окончилась неудачей, указывающей на потерю ключа авторизации для синхронизации между CM и CMTS.

Код: 10

Атрибуты:

Таблица 7-11/J.125 – Атрибуты недействительности авторизации

Атрибут	Содержание
Error-Code	Код ошибки, идентифицирующий причину недействительности авторизации
Display-String (необязательный)	Строка отображения, описывающая условие неудачи

7.2.1.8 Недействительность ключа TEK (TEK Invalid)

Система CMTS посылает сообщение о недействительности TEK клиенту CM, если CMTS определяет, что CM зашифровал пакеты данных PDU в восходящем направлении недействительным ключом TEK; т. е. номер последовательности ключа SAID TEK, содержащийся в элементе расширенного заголовка базовой защиты полученного пакета, находится вне известного CMTS диапазона действующих номеров последовательностей для этого SAID.

Код: 11

Атрибуты:

Таблица 7-12/J.125 – Атрибуты недействительности TEK

Атрибут	Содержание
Key-Sequence-Number	Авторизация номера последовательности ключа
SAID	Ассоциация безопасности ID
Error-Code	Код ошибки, идентифицирующий причину сообщения о недействительности TEK
Display-String (необязательный)	Строка отображения, которая содержит информацию, определяющую поставщика
HMAC-Digest	Сжатое сообщение с материалом распределения и ввода ключей SHA

Атрибут HMAC-Digest – это сжатое сообщение с материалом распределения и ввода ключей. Атрибут HMAC-Digest ДОЛЖЕН быть заключительным атрибутом в списке атрибутов. Сжатое сообщение помещают поверх заголовка сообщения BPKM (начиная с поля кода BPKM) и всех атрибутов недействительности TEK, иных чем HMAC-Digest, в таком порядке, в котором они появляются в пакете

Включение сжатого сообщения с материалом распределения и ввода ключей позволяет принимающему клиенту идентифицировать сообщение недействительности TEK и обеспечивает синхронизацию авторизации ключей CM и CMTS. Ключ идентификации HMAC-Digest находят из ключа авторизации. Подробное описание см. в Разделе 10.

7.2.1.9 Информация идентификации (Authent Info)

Сообщение информация идентификации содержит единственный атрибут CA-Certificate, который включает сертификат CA X.509 производителя. Сертификат X.509 пользователя CM ДОЛЖЕН быть выпущен уполномоченными по сертификации, идентифицированными сертификатом CA X.509. Все сертификаты CA X.509 ДОЛЖНЫ быть выпущены главными уполномоченными по сертификации.

Сообщения с информацией об идентификации являются строго информативными: хотя CM ДОЛЖЕН передавать сообщения с информацией об идентификации, как указывает модель состояния идентификации (пункт 7.1.2), CMTS МОЖЕТ игнорировать эти сообщения.

Код: 12

Атрибуты:

Таблица 7-13/J.125 – Атрибуты информации идентификации

Атрибут	Содержание
CA-Certificate	Сертификат CA производителя, который выпустил сертификат CM

Атрибут CA-Certificate содержит сертификат CA X.509 для CA, который выпустил сертификат пользователя CM X.509. Уполномоченный по сертификации DOCSIS выпускает эти сертификаты CA для производителей CM, которые сертифицированы системой DOCSIS.

7.2.1.10 Запрос отображения SA (MAP Request)

Модем CM отправляет запросы отображения SA в свою систему CMTS, чтобы запросить отображение трафика конкретного потока в нисходящем направлении в SA BPI+. В Разделе 8 описана модель состояния отображения SA. которая использует это сообщение.

Код: 13

Атрибуты:

Таблица 7-14/J.125 – Атрибуты запроса отображения SA

Атрибут	Содержание
CM-Identification	Содержит информацию, которую используют для идентификации кабельного модем в системе CMTS
SA-Query	Содержит адресную информацию, идентифицирующую трафик потока в нисходящем направлении, которую запрашивает CM для отображения SA

7.2.1.11 Ответ на запрос отображения SA (Map Reply)

Система CMTS отправляет ответ на запрос отображения SA в виде положительного ответа на запрос клиента CM. Ответ на запрос отображения SA информирует CM об установлении соответствия (отображении) между запрошенным адресом и SA BPI+. В Разделе 8 описана модель состояния отображения SA, которая использует это сообщение.

Код: 14

Атрибуты:

Таблица 7-15/J.125 – Атрибуты ответа на запрос отображения SA

Атрибут	Содержание
SA-Query	Содержит адресную информацию, идентифицирующую трафик потока в нисходящем направлении, которую запрашивает CM для отображения SA
SA-Descriptor	Составной атрибут дескриптора SA, который определяет отображенный идентификатор SAID SA и другие свойства.

7.2.1.12 Отказ отображения SAID (Map Reject)

Система CMTS отправляет отказ отображения SA в виде отрицательного ответа на запрос клиента CM. Отказ отображения SA информирует CM, что:

1) либо поток трафика в нисходящем направлении, идентифицированный в атрибуте SA-Query, не зашифрован; либо
2) запрашиваемый CM не имеет прав на получение этого трафика.

Содержание атрибута кода ошибки различается для этих двух случаев. В Разделе 8 описана модель состояния отображения SA, которая использует это сообщение.

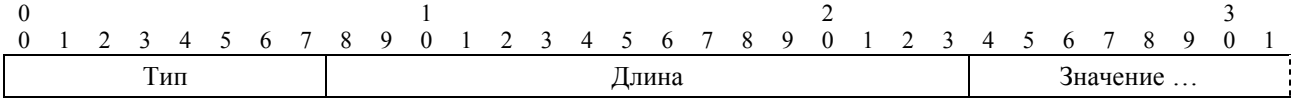
Код: 15

Атрибуты:

Таблица 7-16/J.125 – Атрибуты отказа отображения SA

Атрибут	Содержание
SA-Query	Содержит адресную информацию, идентифицирующую трафик потока в нисходящем направлении, которую запрашивает CM для отображения SA
Error-Code	Код ошибки, который идентифицирует причину отказа на запрос отображения SA
Display-String (необязательный)	Строка отображения на экран причины отказа

7.2.2 Атрибуты BPKM



Итоговая сводка формата атрибута показана ниже. Поля передают слева направо.

Тип:

Тип поля – это один октет. Значения типов полей BPKM определены ниже.

ПРИМЕЧАНИЕ 1. – Значения типов от 0 до 127 определены в спецификации базовой защиты, а значения от 128 до 255 – это типы атрибутов, присвоенные производителем.

Сервер BPKM ДОЛЖЕН игнорировать атрибуты неизвестных типов.

Клиент BPKM ДОЛЖЕН игнорировать атрибуты неизвестных типов.

Клиент и сервер BPKM (т. е. CM и CMTS) МОГУТ записать атрибуты неизвестных типов.

Таблица 7-17/J.125 – Типы атрибутов BPKM

Тип	Атрибут BPKM
0	Зарезервирован
1	Serial-Number
2	Manufacturer-ID
3	MAC-Address
4	RSA-Public-Key
5	CM-Identification
6	Display-String
7	AUTH-KEY
8	TEK
9	Key-Lifetime
10	Key-Sequence-Number
11	HMAC-Digest
12	SAID
13	TEK-Parameters
14	OBSOLETED
15	CBC-IV

Таблица 7-17/J.125 – Типы атрибутов BPKM

Тип	Атрибут BPKM
16	Error-Code
17	CA-Certificate
18	CM-Certificate
19	Security-Capabilities
20	Cryptographic-Suite
21	Cryptographic-Suite-List
22	BPI-Version
23	SA-Descriptor
24	SA-Type
25	SA-Query
26	SA-Query-Type
27	IP-Address
28	Download-Parameters
29-126	Зарезервировано
127	Vendor-Defined
128-255	Vendor-assigned attribute types

Длина

Поле длины составляет 2 октета и указывает длину в октетах этого значения поля атрибута. Поле длины не включает тип и длину поля[5]. Минимальная длина этого атрибута равна 0, а максимальная равна 1487.

Пакеты, содержащие атрибуты с недействительными длинами СЛЕДУЕТ спокойно отбрасывать.

Значение

Поле значения равно нулю или более октетов и содержит информацию специфики атрибута. Формат и длина поля значения определяется полями типа и длины. Все величины из многих октетов располагаются в порядке байтов сети, т. е. октет, который содержит наиболее значащий бит, передают в сеть первым.

ПРИМЕЧАНИЕ 2. – "Строка" не требует окончания NULL ASCII, поскольку этот атрибут уже имеет поле длины.

Формат поля значения является одним из пяти типов данных.

[5] Это важно как при кодировании TLV, которое используют в элементах расширенных заголовков MAC RF, так и при кодировании TLV, которое используют в установках конфигурации файла конфигурации CM [J.112-B] или [J.122]. Кодирование TLV BPKM отличается от кодирования по протоколу RADIUS, в котором структура основного сообщения BPKM основана на поле длины атрибутов RADIUS и которое включает поля типа и длины, а также поле значения атрибута.

Таблица 7-18/J.125 – Типы атрибутов значения данных

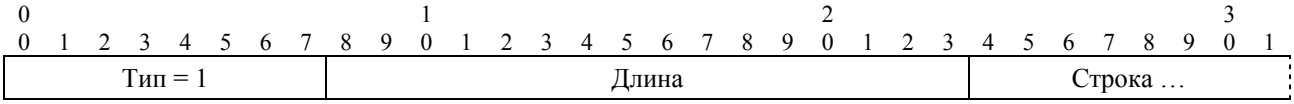
string	0-1487 октетов
uint8	8 битов целого без знака
uint16	16 битов целого без знака
uint32	32 бита целого без знака
compound	Набор атрибутов

7.2.2.1 Серийный номер (Serial-Number)

Описание

Этот атрибут указывает серийный номер, присвоенный производителем кабельному модемному устройству.

Итоговый формат атрибута "Серийный номер" показан ниже. Поля передают слева направо.



Тип

1 для серийного номера

Длина

≥0 и ≤255

Строка

Поле строк равно нулю или более октетов и содержит серийный номер, присвоенный производителем.

Серийный номер, присвоенный производителем, ДОЛЖЕН быть закодирован знаками кодирования ISO/IEC 8859-1. Используемые знаки ДОЛЖНЫ быть ограничены следующим:

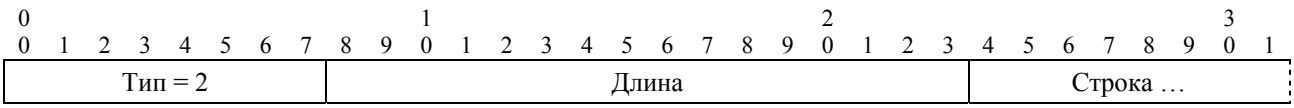
- A-Z (0x41-0x5A)
- a-z (0x61-0x7A)
- 0-9 (0x30-0x39)
- "-" (0xD2)

7.2.2.2 Идентификатор ID производителя (Manufacturer-ID)

Описание

Этот атрибут идентифицирует производителя. Длина идентификатора составляет 3 октета и содержит 3-х октетный организационно единственный идентификатор (OUI), предназначенный IEEE [IEEE1] для использования организациями. Первые два бита 3-октетной строки устанавливают на нуль.

Итоговый формат атрибута "ID производителя" показан ниже. Поля передают слева направо.



Тип

2 для ID производителя

Длина

3

Строка

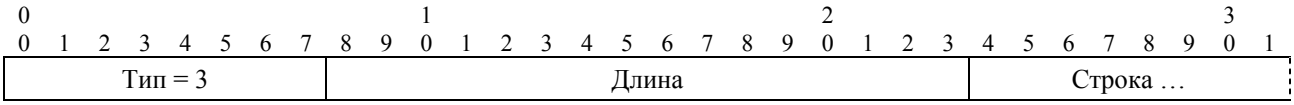
Поле строки составляет три октета и содержит IEEE OUI.

7.2.2.3 MAC-адрес (MAC-Address)

Описание

Этот атрибут идентифицирует MAC адрес IEEE, присвоенный CM. Для гарантии его единственности, проще всего обработать в CMTS индекс кабельного модема.

Итоговый формат атрибута "MAC-адрес" показан ниже. Поля передают слева направо.



Тип

3 для MAC-адреса

Длина

6

Строка

Поле строки содержит 6-ти октетный MAC адрес.

7.2.2.4 Открытый ключ RSA (RSA-Public-Key)

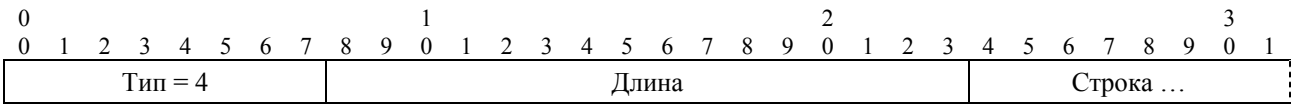
Описание

Этот атрибут является строкой атрибута, содержащего кодированный по типу ASN.1 DER открытый ключ RSAPublicKey, как это определено в стандарте шифрования RSA PKCS № 1 v2.0 [RSA3].

Стандарт PKCS № 1 v2.0 определяет, что открытый ключ RSA состоит как из открытых модулей RSA, так и из открытого расширения RSA. Тип RSAPublicKey включает оба эти типа ЦЕЛИКОМ, кодированные методом DER.

Стандарт состояний PKCS № 1 v2.0 определяет, что открытое расширение RSA МОЖЕТ быть стандартизовано для особых приложений и предлагает значения 3 или 65537 (F4). Базовая защита плюс стандартизирует по F4 открытое расширение и использует 1024-битовые модули (базовая защита использует 768-битовые модули). Чтобы сделать возможным обновление программ DOCSIS 1.0 для оборудования BPI+, применения BPI+ ДОЛЖНЫ поддерживать 768-битовые модули.

Итоговый формат атрибута "Открытый ключ" показан ниже. Поля передают слева направо.



Тип

4 для открытого ключа RSA

Длина

106, 140 или 270 (при длине кодирования DER использует F4 как открытое расширение и 768-битовый, 1024-битовый или 2048-битовый открытый модуль соответственно)

Строка

Тип кодирования DER RSAPublicKey ASN.1

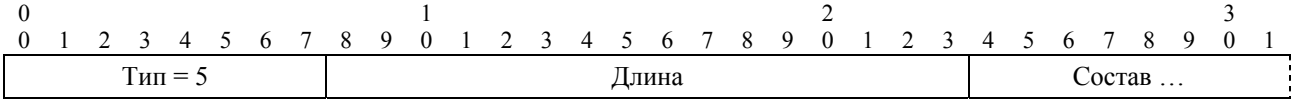
7.2.2.5 Идентификация CM (CM-Identification)

Описание

Этот атрибут является составным, состоящим из набора податрибутов. Эти податрибуты содержат информацию, которую можно использовать, чтобы однозначно идентифицировать кабельный модем. Податрибуты ДОЛЖНЫ включать:

- Серийный номер;
- ID производителя;
- MAC-адрес;
- Открытый ключ RSA.

Идентификация CM МОЖЕТ также содержать необязательные атрибуты, определенные производителем.



Тип

5

Длина

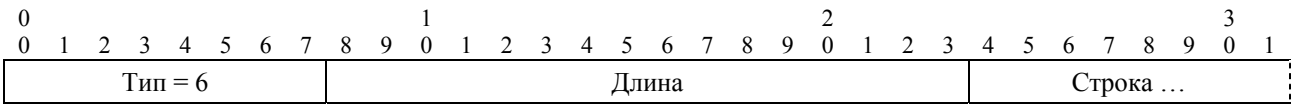
≥126

7.2.2.6 Строка отображения (Display-String)

Описание

Этот атрибут содержит текстовое сообщение. Обычно его используют для объяснения неудачи ответа. Этот атрибут может быть записан приемником, чтобы в дальнейшем его мог найти менеджер SNMP. Строки отображения ДОЛЖНЫ быть не более 128 байтов.

Итоговый формат атрибута "Строка отображения" показан ниже. Поля передают слева направо.



Тип

6 для строки отображения

Длина

≥0 и ≤128

Строка

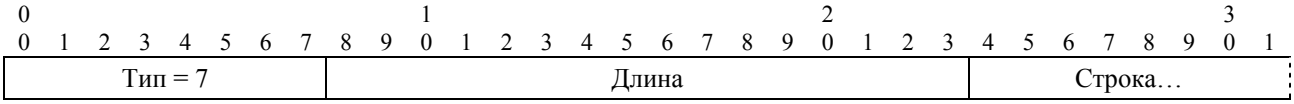
Строка знаков. Не существует требования, согласно которому строка знаков должна оканчиваться нулем. Поле длины всегда идентифицирует конец строки.

7.2.2.7 Ключ AUTH (AUTH-Key)

Описание

Ключ авторизации составляет 20 байтов, из которых находят ключ шифрования ключей и два ключа идентификации сообщения (один для запросов в восходящем направлении, а другой для ответов в нисходящем направлении).

Этот атрибут состоит либо из 96, либо из 128 октетов, содержащих ключ авторизации, зашифрованный RSA с помощью открытого ключа СМ 768 битами или 1024 битами RSA. Подробности процедуры шифрования RSA приведены в 10.5. Зашифрованный по алгоритму RSA текст должен иметь длину модулей RSA, т. е. либо 96, либо 128 октетов.



Тип

7 для ключа AUTH

Длина

96 или 128

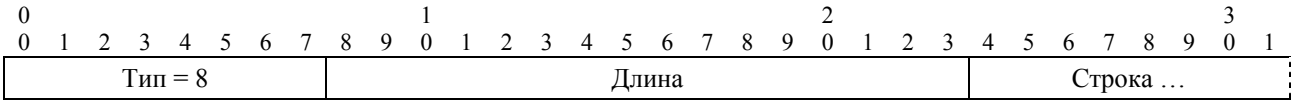
Строка

96 или 128 октетов, представляющая зашифрованный RSA ключ авторизации.

7.2.2.8 TEK

Описание

Этот атрибут содержит 8 октетов, которые представляют ключ DES TEK, зашифрованный ключом шифрования ключей, который находят из ключа авторизации. Ключи TEK шифруют, используя режим двух ключевого тройного алгоритма DES шифрование–расшифрование–шифрование (EDE). Подробности см. в Разделе 10.



Тип

8 для TEK

Длина

8

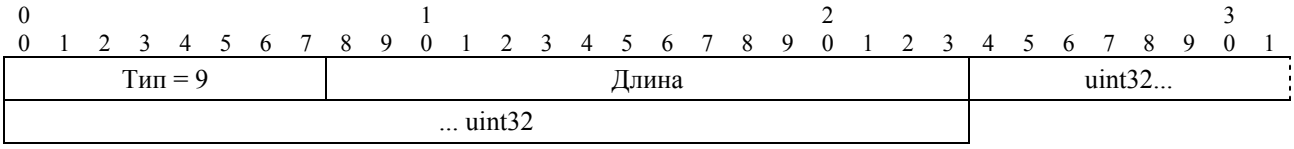
Строка

64 битов, представляющих (режим двух ключевого тройного алгоритма DES EDE) зашифрованный ключ шифрования трафика.

7.2.2.9 Срок жизни ключа (Key-Lifetime)

Описание

Этот атрибут содержит срок жизни (в секундах) ключа авторизация или ключа TEK. Атрибут – это 32 бита, выражающих целое без знака и представляющих время в секундах, в течение которого ключ еще будет действующим.



Тип

9 для срока жизни ключа

Длина

4

uint32

32 бита, представляющих срок жизни ключа

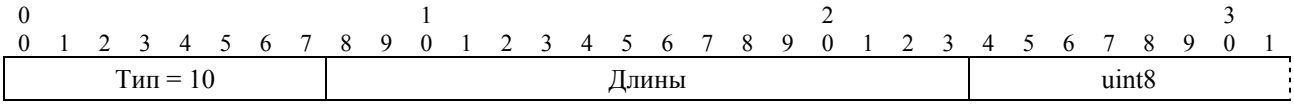
Срок жизни ключа нуль указывает, что соответствующие ключи авторизация или шифрования трафика более не действуют.

7.2.2.10 Номер последовательности ключа (Key-Sequence-Number)

Описание

Этот атрибут содержит 4 бита номера последовательности для ключа TEK или авторизации. Однако эти 4 бита хранят в одном октете с установкой на нуль 4 битов высокого порядка.

Итоговый формат атрибута "Номер последовательности ключа" показан ниже. Поля передают слева направо.



Тип

10 для номера последовательности ключей

Длины

1

uint8

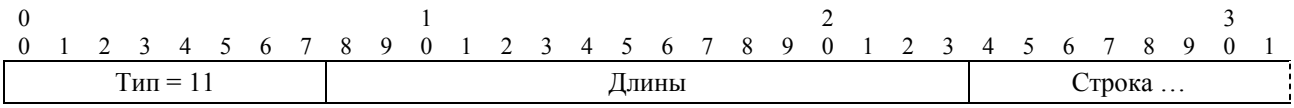
4 бита номера последовательности

7.2.2.11 Сжатое сообщение с материалом распределения и ввода ключей HMAC (HMAC-Digest)

Описание

Этот атрибут содержит хэш с материалом распределения и ввода ключей, который используют для сообщения идентификации. Алгоритм HMAC определен в [RFC2104] с использованием обычного криптографического хэш алгоритма. Базовая защита использует конкретные версии HMAC, которые применяют. Алгоритм хэш защиты (SHA-1), описан в [FIPS-180-2].

Итоговый формат атрибута "HMAC-Digest" показан ниже. Поля передают слева направо.



Тип

11 для HMAC-Digest

Длина

20 октетов

Строка

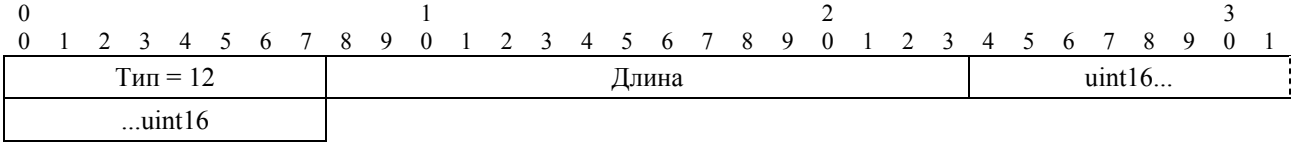
160 битов (20 октетов) материала распределения и ввода ключей хэш SHA

7.2.2.12 SAID

Описание

Этот атрибут содержит 14 битов ID ассоциации безопасности (SAID), использованные базовой защитой плюс в качестве идентификатора ассоциации безопасности. Два бита высшего порядка устанавливают на нуль.

ПРИМЕЧАНИЕ. – Первичный SAID BPI+ CM равен первичному SID этого CM.



Тип

12 для SAID

Длина

2

uint16

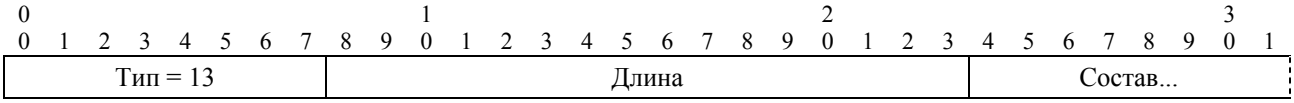
16 битов, представляющих SAID.

7.2.2.13 Параметры TEK (TEK-Parameters)

Описание

Этот атрибут – составной и состоит из набора податрибутов. Податрибуты представляют все параметры защиты, связанные с конкретной генерацией ключа TEK SAID.

Итоговый формат атрибута "Параметры TEK" показан ниже. Поля передают слева направо.



Тип

13 для параметров TEK

Длина

33

Состав

Поле состава содержит следующие податрибуты:

Таблица 7-19/J.125 – Податрибуты TEK-Parameters

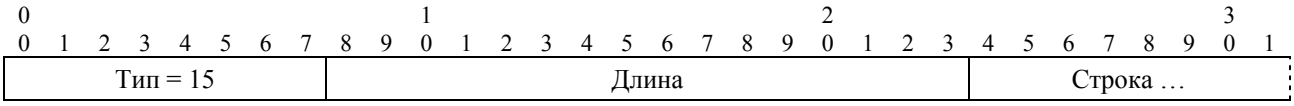
Атрибут	Содержание
TEK	TEK, зашифрованный (режим режим двух ключевого тройного алгоритма DES-EDE) с помощью KEK
Key-Timelife	Оставшийся срок жизни TEK
Key-Sequence-Number	Номер последовательности TEK
CBC-IV	Вектор инициализации соединенного блока шифрования (CBC)

7.2.2.14 CBC-IV

Описание

Этот атрибут содержит 64-битовое (8-октетов) значение, определенное в векторе инициализации соединенного блока шифрования (CBC).

Итоговый формат атрибута "CBC-IV" показан ниже. Поля передают слева направо.



Тип

15 для CBC-IV

Длина

8 октетов

Строка

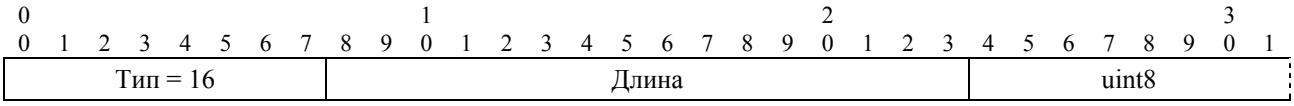
64-х битовая величина представляет вектор инициализации DES-CBC.

7.2.2.15 Код ошибки (Errror-Code)

Описание

Этот атрибут содержит один октет кода ошибки, который дает дополнительную информацию об отказе в авторизации, отказе в ключе, недействительности авторизации или недействительности TEK.

Итоговый формат атрибута "Код ошибки" показан ниже. Поля передают слева направо.



Тип

16 для кода ошибки

Длина

1

uint8

1 октет кода ошибки

Система CMTS ДОЛЖНА включить атрибут код ошибки во все сообщения отказов на авторизацию, недействительности авторизации, отказов в ключе, недействительности TEK и отказов SA-MAP Reject. В таблице 7-20 перечислены значения кодов для использования с этим атрибутом. Система CMTS ДОЛЖНА использовать перечисленные ниже ненулевые коды ошибок сообщений отказов в отображении SA-MAP. Система CMTS МОЖЕТ использовать перечисленные ниже ненулевые коды ошибок для других типов сообщений BPI+. Однако, система также МОЖЕТ возвратить значение кода нуль (0). Значения кодов ошибки иные, чем те, которые описаны в таблице 7-20, ДОЛЖНЫ игнорироваться. При возвращении кода с нулевым значением, не передают дополнительную информацию о неудаче CM. Это МОЖЕТ быть желательно по причинам защиты.

Таблица 7-20/J.125 – Значения кодов атрибута Errror-Code

Код ошибки	Сообщения	Описание
0	Все	Нет информации
1	Auth Reject, Auth Invalid	Не авторизован CM
2	Auth Reject, Key Reject	Не авторизован SAID
3	Auth Invalid	Добровольный
4	Auth Invalid, TEK Invalid	Недействительность номера последовательности ключей
5	Auth Invalid	Сообщение (запрос ключа) идентификации неудачи
6	Auth Reject	Долговременная неудача авторизации
7	Map Reject	Нет авторизации для запрошенного в нисходящем направлении потока трафика
8	Map Reject	В нисходящем направлении поток трафика не отображен в SAID BPI+
9	Auth Reject	Не получено время для работы

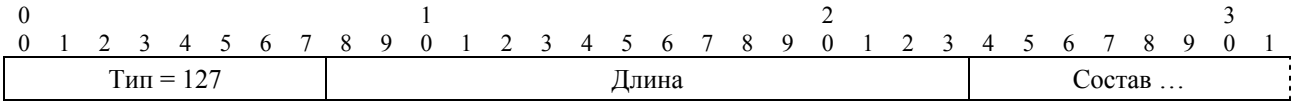
Код ошибки 6, долговременная неудача авторизации, используют для указания на число различных ошибочных условий, влияющих на обмен при авторизации BPKM. Эти условия включают:

- неизвестный производитель; т. е. CMTS не имеет сертификата CA, принадлежащего лицу, выпустившему в обращение сертификат CM;
- подпись сертификата CM недействительна;
- неудача анализа ASN.1 во время проверки сертификата CM;
- сертификат CM находится в "горячем списке";
- несоответствия между данными сертификата и данными в сопроводительных атрибутах BPKM;
- CM и CMTS имеют несовместимые возможности защиты.

Их общее свойство заключается в том, что условие неудачи рассматривается как долговременные: любые новые попытки авторизации могли бы закончиться отказом в авторизации. Подробности о случае долговременной неудачи авторизации МОГУТ быть сообщены CM в необязательном атрибуте строки отображения, которая МОЖЕТ сопровождать атрибут код ошибки в сообщениях отказа на авторизацию. Если дополнительные детали отправляют в CM, то системе CMTS СЛЕДУЕТ обеспечить возможность административного управления. Система CMTS МОЖЕТ записать эти неудачи авторизации или даже перехватывать их для администратора SNMP.

7.2.2.16 Определенный поставщиком атрибут (Vendor-Defined)

Определенный поставщиком атрибут является составным, у которого первый податрибут ДОЛЖЕН быть атрибутом идентификатора ID производителя. Последующие атрибуты определяются пользователем со значениями типов, присвоенными поставщиком и идентифицированные атрибутом ID производителя.



Тип

127 для определенного поставщиком

Длина

≥6

Состав

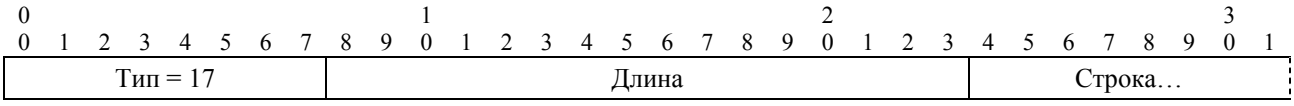
Первый податрибут ДОЛЖЕН быть ID производителя. Последующие атрибуты могут включать как универсальные типы (т. е. определенные этой Рекомендацией), так и типы, определенные поставщиком, специфические для поставщика и идентифицированные в предшествующем податрибуте ID производителя.

7.2.2.17 Сертификат CA (CA-Certificate)

Описание

Этот атрибут является строкой атрибута, содержащего сертификат CA X.509, как это описано в [X.509].

Итоговый формат атрибута "Сертификат CA" показан ниже. Поля передают слева направо.



Тип

17 для сертификата CA

Длина

Переменная. При превышении допустимого размера, длина НЕ ДОЛЖНА стать причиной вызова сообщения управления MAC.

Строка

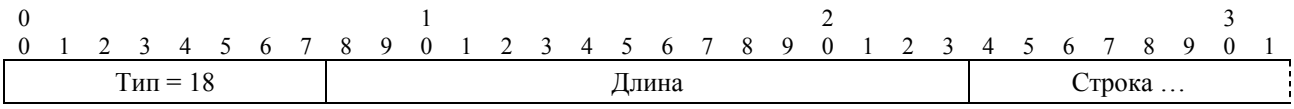
Сертификат CA X.509 (кодированный DER ASN.1)

7.2.2.18 Сертификат CM (CM-Certificate)

Описание

Этот атрибут является строкой атрибута, содержащего сертификат X.509 пользователя кабельного модема, как описано в [X.509].

Итоговый формат атрибута "Сертификат CM" показан ниже. Поля передают слева направо.



Тип

18 для сертификата CM

Длина

Переменная. При превышении допустимого размера, длина НЕ ДОЛЖНА стать причинной вызова сообщения управления MAC.

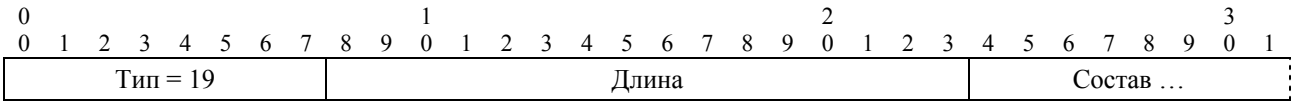
Строка

Сертификат пользователя X.509 (кодированный DER ASN.1)

7.2.2.19 Возможности защиты (Security-Capabilities)

Описание

Атрибут "Возможности защиты" является составным атрибутом, податрибуты которого идентифицируют версии BPI+, которые поддерживает CM, и криптографические наборы, которые поддерживает CM.



Тип

19 для возможностей защиты

Длина

≥9

Состав

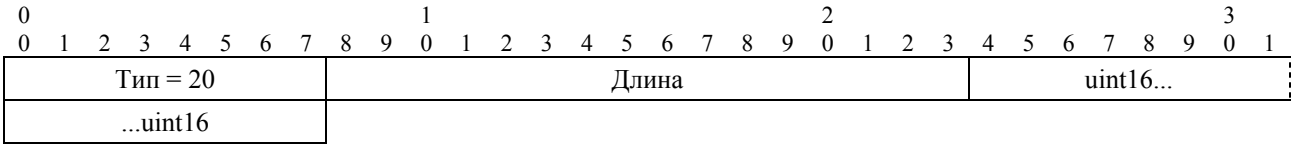
Поле состав содержит следующие податрибуты:

Таблица 7-21/J.125 – Податрибуты Security-Capabilities

Атрибут	Содержание
Cryptographic-Suite-List	Список поддерживаемых криптографических наборов
BPI-Version	Версии, поддерживаемые BPI+

7.2.2.20 Криптографический набор (Cryptographic-Suite)

Описание



Тип

20 для криптографического набора

Длина

2

uint16

16-ти битовое целое, идентифицирующее спаривание алгоритма шифрования данных (кодированных слева направо с наиболее значащим байтом) и алгоритма идентификации данных (кодированных справа налево с наименее значащим байтом). В настоящее время алгоритмы DES 56-битовый и 40-битовый являются единственными алгоритмами, определенными для использования в защите DOCSIS, и не существует никаких парных алгоритмов идентификации данных.

Таблица 7-22/J.125 – Идентификаторы алгоритмов шифрования данных

Значение	Описание
0	Зарезервировано
1	CBC-Mode, 56-битовый DES
2	CBC-Mode, 40-битовый DES
3-255	Зарезервировано

Таблица 7-23/J.125 – Идентификаторы алгоритмов идентификации данных

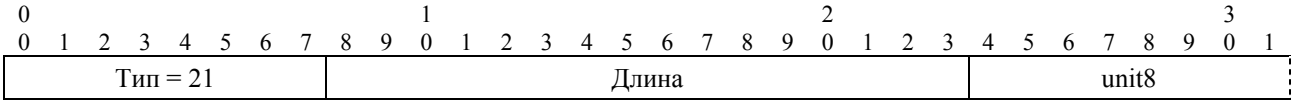
Значение	Описание
0	Отсутствует идентификация данных
1-255	Зарезервировано

Таблица 7-24/J.125 – Значение атрибута Cryptographic-Suite

Значение	Описание
256 (0x0100 hex)	CBC-Mode 56-битовый DES. Нет идентификации данных
512 (0x0200 hex)	CBC-Mode 40-битовый DES. Нет идентификации данных
Все оставшиеся значения	Зарезервировано

7.2.2.21 Список криптографического набора (Cryptographic-Suite-List)

Описание



Тип

21 для списка криптографического набора

Длина

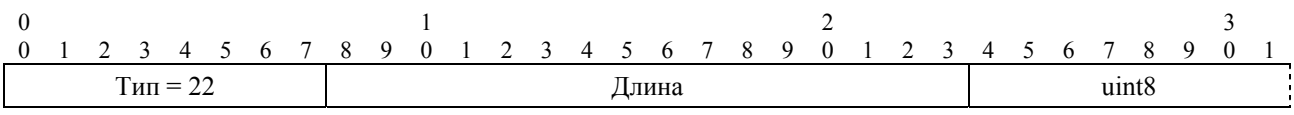
2 × n, где n = числу перечисленных криптографических наборов

unit8

Список пар байтов, идентифицирующих комплекты криптографических наборов. Каждая пара байтов представляет поддерживаемый криптографический набор с кодированием, соответствующим значению поля атрибута "Список криптографического набора" (см. 7.2.2.20). Система CMTS НЕ ДОЛЖНА интерпретировать относительный порядок в списке пар байтов как предпочтение, которое CM отдает этому криптографическому набору перед другими, которые поддерживает система.

7.2.2.22 Версия BPI (BPI-Version)

Описание



Тип

22 для BPI-Version

Длина

1

uint8

1 октет кода, идентифицирующего версию базовой защиты.

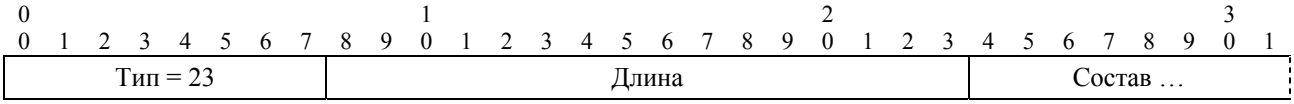
Таблица 7-25/J.125 – Значения атрибутов BPI-Version

Значение	Описание
0	Зарезервировано
1	BPI+
2-255	Зарезервировано

7.2.2.23 Дескриптор SA (SA-Descriptor)

Описание

Атрибут "Дескриптор SA" является составным атрибутом, податрибуты которого описывают свойства ассоциации безопасности BPI+. Эти свойства включают SAID, тип SA и криптографический набор, который используют с SA.



Тип

23 для дескриптора SA

Длина

14

Состав

Поле состава содержит следующие податрибуты:

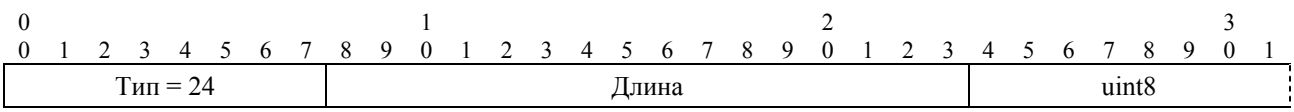
Таблица 7-26/J.125 – Податрибуты SA-Descriptor

Атрибут	Содержание
SAID	ID ассоциации безопасности
SA-Type	Тип SA
Cryptographic-Suite	Спаривание алгоритмов шифрования данных и идентификации данных, используемых в SA.

7.2.2.24 Тип SA (SA-Type)

Описание

Идентифицирует тип SA. BPI+ определяет три типа SA: первичный, статический, динамический.



Тип

24 для типа SA

Длина

1

uint8

1 октет кода, идентифицирующего значение типа SA, как описано в таблице 7-27.

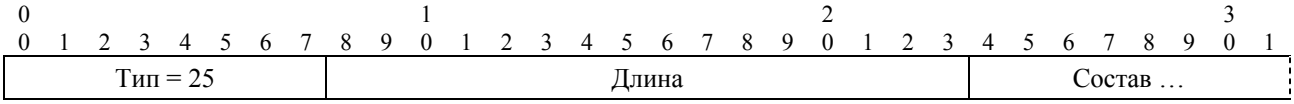
Таблица 7-27/J.125 – Значения атрибутов SA-Type

Значение	Описание
0	Первичный
1	Статический
2	Динамический
3-127	Зарезервировано
128-255	Особые поставщика

7.2.2.25 Запрос SA (SA-Query)

Описание.

Составной атрибут, используемый в запросе отображения SA Map для определения аргументов запроса отображения. Аргументы запроса включают запрос типа и любые атрибуты адресации, специфические для данного типа запроса – атрибуты адресации идентифицируют конкретный поток трафика в нисходящем направлении, отображение которого запрашивает SA. В настоящее время единственным определенным типом является IP-Multicast (многоадресная передача по сети IP), а аргументом адресации – связанный с этим типом групповой адрес IP.



Тип

25 для запроса SA

Длина

11

Состав

Поле состава содержит следующие податрибуты:

Таблица 7-28/J.125 – Податрибуты SA-Query

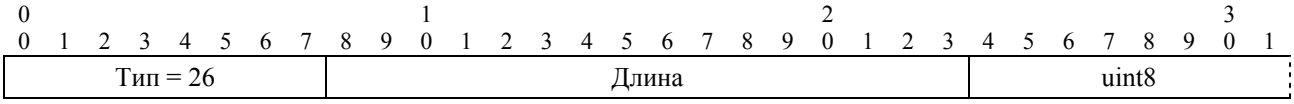
Атрибут	Содержание
SA-Query-Type	Тип запроса
IP-Address	Требуется, если SA-Query-Type = IP-Multicast; содержит групповой адрес IP, отображение SA которого запрашивают.

7.2.2.26 Тип запроса SA (SA-Query-Type)

Описание

Этот атрибут идентифицирует IP адрес, который используют для идентификации зашифрованного потока трафика IP. Например, этот атрибут используют для описания адреса при многоадресной групповой передаче по IP.

Итоговый формат атрибута "SA-Query-Type" показан ниже. Поля передают слева направо.



Тип

26 для SA-Query-Type

Длина

1

uint8

1 октет кода, идентифицирующего значение SA-Query-Type, как описано в таблице 7-29.

Таблица 7-29/J.125 – Значения атрибутов SA-Query-Type

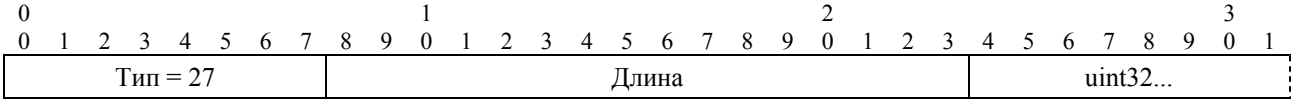
Значение	Описание
0	Зарезервировано
1	Многоадресная передача по протоколу IP
2-127	Зарезервировано
128-255	Особые поставщика

7.2.2.27 IP адрес (IP-Address)

Описание

Этот атрибут идентифицирует IP адрес, который используют для идентификации зашифрованного потока трафика IP. Например, этот атрибут используют при многоадресной групповой передаче по IP.

Итоговый формат атрибута "IP-адрес" показан ниже. Поля передают слева направо.



Тип

27 для IP-адреса

Длина

4

uint32

Содержит 32 бита целого числа без знака (в сетевом порядке байтов), представляющих IP адрес.

7.2.2.28 Параметры загрузки (Download-Parameters)

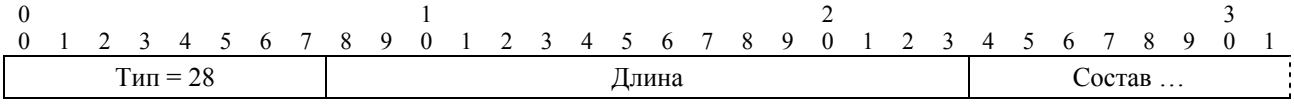
Описание

Этот атрибут используют в файле кода CM, описанного в B.3.1. Этот атрибут является составным, состоящим из набора податрибутов.

Податрибут МОЖЕТ включать один или более следующих атрибутов в указанном порядке:

- Открытый ключ RSA (нуль или один);

- Сертификат CA (нуль, один или более).



Тип

28

Длина

≥0

8 Отображение динамической SA

8.1 Введение

Динамические ассоциации безопасности (динамические SA) BPI+, введенные в 5.1.3, являются SA, которые CMTS устанавливает и исключает динамически в ответ на запрос о включении или выключении потоков трафика в нисходящем направлении. Эти потоки трафика могут быть инициированы действием следующих устройств:

- устройством CPE (оборудование в помещении пользователя), присоединенным к одному из клиентов CM системы CMTS;
- сервером приложения в головном узле;
- системой OSS;
- другими, неперечисленными здесь устройствами.

Независимо от того, что служит источником установления динамической SA в CMTS, клиенты CM нуждаются в механизме обучения отображения конкретного BPI+ с защищенным в нисходящем направлении потоком трафика в такой же поток, динамически присвоенный BPI+ ассоциации безопасности (и такие же SA, соответствующие SAID).

Машина состояния отображения SA, описанная в этом разделе, определяет, каким образом кабельные модемы запрашивают у CMTS отображение потоков трафика нисходящем направлении в динамические SA. Машина состояния управляет передачей запросов сообщений Map SA в систему CMTS.

В настоящее время DOCSIS 1.1 или DOCSIS 2.0 используют динамические SA для единственного типа: шифрования и тем самым ограничения доступа к многоадресному IP трафику в нисходящем направлении. Система CMTS может установить или исключить динамические SA в ответ на изменения членов группы IP устройств CPE в нисходящем направлении. Механизмы управления DOCSIS 1.1 или 2.0 IGMP ([J.112-B] пункт B.5.3.1 или [J.122] пункт 5.3.1), могут инициировать установление динамических SA в CMTS. Механизмы управления IGMP в CM ДОЛЖНЫ инициировать запросы сообщений отображения Map BPI+, которые поступают от CMTS для отображения адреса группы SA при многоадресной рассылке.

Механизм отображения SA BPI+ МОЖЕТ отображать группу многоадресной рассылки в статический SA или даже в конкретную первичную SA CM. Ответ CMTS на запрос отображения может возвратить три типа SA. Однако механизм отображения SA является единственным механизмом, с помощью которого CM может получить информацию о динамических SA.

В пункте 8.4 будет обсуждаться более подробно конкретное использование механизма отображения SA для поддержки отображения многоадресного трафика IP в динамические SA. Однако в следующих двух разделах внимание будет сфокусировано на более общем механизме отображения SA.

ПРИМЕЧАНИЕ. – В будущих расширениях спецификаций служб DOCSIS будут описаны дополнительные приложения динамических SA.

8.2 Теория операции

BPI+ определяет три новых сообщения BPKM для поддержания запроса CM на отображения SA: запросы SA Map, SA Map Reply и SA Map Reject. Модем CM отправляет запрос Map в CMTS для запроса отображения в SA известного потока в нисходящем направлении. Запрос Map несет атрибуты данных BPI+, идентифицирующие запрашиваемый CM, и поток трафика в нисходящем направлении, отображение которого запрашивают SA.

Система CMTS ДОЛЖНА ответить на запросы Map *одним из двух сообщений*:

- Map Reply, передающее модему CM запрошенное отображение SA; *или*
- Map Reject, сигнализирующее модему CM, что:
  1) либо CM не авторизован на получение потока трафика, идентифицированного в запросе Map; либо
  2) запрошенный поток трафика не отображен в SA интерфейса BPI+.

Если CM не получает никакой из этих ответов за настраиваемый период времени ожидания, он вновь посылает запрос Map. Если ответ не получен после максимального настроенного числа повторов запросов, модем CM прекращает запросы.

Если CM получает отказ в отображении (Map Reject), он прекращает все дальнейшие попытки получить отображение. В случае, если доступ к потоку трафика в нисходящем направлении отображен в SA BPI+, а запрашиваемый CM не авторизован на доступ к этой SA, модему CM и закрепленному за ним устройству CPE будет отказано в доступе, т. к. CM не сможет получить материал распределения и ввода ключей, необходимый для расшифровки потоков трафика в нисходящем направлении, зашифрованных в соответствии с данной SA. Например, пользователь может запрашивать более дорогую услугу, на которую он или она не подписаны. В случае если запрошенный поток трафика не зашифрован (т. е. он не отображен в SA), незашифрованный трафик будет просто направлен к присоединенному устройству CPE. Например, CM делает запрос SA-MAP адресов всех многоадресных хостов. Поскольку все многоадресные пакеты, адресованные всем многоадресным хостам, необходимы для соответствующей работы IGMP, нет необходимости шифровать эти пакеты.

Если CM получает ответ (Map Reply). идентифицирующий SA BPI+, связанную с запрошенным потоком трафика в нисходящем направлении, CM запускает машину состояния TEK для данной SA, при двух условиях:

1) CM еще не использует машину состояния TEK для данного SA; и
2) CM поддерживает криптографический набор, идентифицированный в ответе на запрос отображения (Map Reply) вместе со значением идентификатора ID ассоциации безопасности (SAID).

Модем CM может уже использовать машину состояния TEK, если отображенная SA это:

- динамическая SA, отображенная в другой защищенный поток трафика, к которому CM уже имеет доступ;
- запрашиваемая первичная SA CM;
- статическая SA, о которой CM получил информацию в ранее полученном ответе на авторизацию.

Система CMTS МОЖЕТ присвоить множеству потоков трафика (т. е. групповым адресам IP) одну и ту же SA. Если более чем один поток трафика в нисходящем направлении зашифрован той же самой динамической SA, модем CM может уже использовать машину состояния TEK для идентифицированной SA в ответе на отображение (Map Reply). Отображенной SA, возвращенной в ответе (Map Reply), не требуется быть типом динамической SA: запрошенный поток трафика может быть отображен в первичную SA или статическую SA модема CM.

Ответ Map Reply включает атрибут дескриптор SA, который идентифицирует как SAID, так и криптографический набор, который используют в SA. Как и в случае статических SA, выбор криптографического набора динамической SA обычно делают независимо от запрашиваемых криптографических возможностей CM. Таким образом, система CMTS МОЖЕТ ответить на запрос отображения ассоциацией SA (либо статической, либо динамической), использующей криптографический набор, который не поддерживает запрашивающий CM. Модем CM НЕ ДОЛЖЕН запускать машину состояния TEK для статических или динамических SA, криптографические наборы которых CM не поддерживает. (Однако первичная SA должна использовать криптографические наборы, поддерживаемыми модемами CM, к которым относятся эти SA).

Машина состояния TEK управляет поиском отображенного материала распределения и ввода ключей SA. Модем CM должен отправить запросы ключей для SA. Система CMTS ДОЛЖНА ответить на эти запросы ключей одним из следующих действий:

- ответить на запрос ключа, поставляя модему CM запрошенный материал распределения и ввода ключей;
- отказать в ключе, сигнализируя CM, что этот модем не имеет прав на запрошенный отображенный идентификатор SAID;
- недействительностью авторизации, сигнализируя CM, что идентификация сообщения запроса ключа потерпела неудачу.

Прием отказа в ключе форсирует завершение машины состояния TEK.

Имеется два механизма для CMTS известить клиента CM, что он не авторизован для доступа к отдельным потокам трафика: ответить на запрос отображения отказом отображения (Map Reject) и ответить на запрос отображения отказом ключа (Key Reject). Их использование зависит от того, проверяет ли CMTS статус авторизации CM до ответа на запрос отображения. При проверке во время обмена отображениями, следует предотвратить возможность запуска без необходимости модемом CM машины состояния TEK и отправку запроса ключа, на который SAID не имеет прав (не авторизован).

8.3 Модель состояния отображения SA

Модель состояния отображения SA определяет механизм, с помощью которого CM получает информацию об отображении потока трафика в динамическую SA.

Машина состояния запускается, когда событие в CM, внешнее по отношению к модели состояния отображения SA, инициирует необходимость в отображении потока трафика в SA (например, когда CM инсталлирует фильтры разрешения для групповой многоадресной рассылки IP в результате действия механизмов управления IGMP CM). Это внешнее событие генерирует внутреннее событие "Map" ("отобразить") в машине состояния отображения SA.

Машина состояния заканчивается, если CM не получает ответа после отправки максимального числа повторений, или когда CM определяет, что более не требуется отображенного материала распределения и ввода ключей SA. В последнем случае, внешнее событие генерирует внутреннее событие "Unmap" ("не отображать") в машине состояния отображения SA, форсируя ее завершение. Таким образом, машину состояния можно использовать не только, чтобы получить требуемую информацию отображения, но также, чтобы отследить период, в течение которого внешнее приложение, используя механизм отображения SA (например, управление IGMP), требует это отображение. Связь события Unmap с внешним событием и, следовательно, использование события Unmap не является ОБЯЗАТЕЛЬНЫМ.

Как и в случаях авторизации BPI+ и машин состояния TEK, машина состояния отображения SA представлена в графическом формате в качестве модели состояния потока (рисунок 8-1), а также в формате таблицы как матрица перехода (таблица 8-1). Что касается ранее описанных машин состояний, то матрица перехода состояний ДОЛЖНА использоваться как определенная спецификация протокола действий, связанных с каждым состоянием перехода.

Если при механизме отображения SA, модем CM получит информацию, что требуется доступ к материалу распределения и ввода ключей динамической SA, модем ДОЛЖЕН установить машину состояния TEK для этой динамической SA. Хотя машина состояния авторизации управляет установлением и завершением машин состояния TEK, связанных с первичной и любыми статическими SAID, эта машина не управляет установлением и завершением машин состояния TEK, связанных с динамическими SA. Модемы CM ДОЛЖНЫ использовать необходимую логику, чтобы установить и завершить машины состояния TEK для динамических SA, получивших информацию от механизма отображения SA. Спецификация BPI+, однако, не описывает, каким образом модемам CM СЛЕДУЕТ управлять их машинами состояния TEK динамических SA.

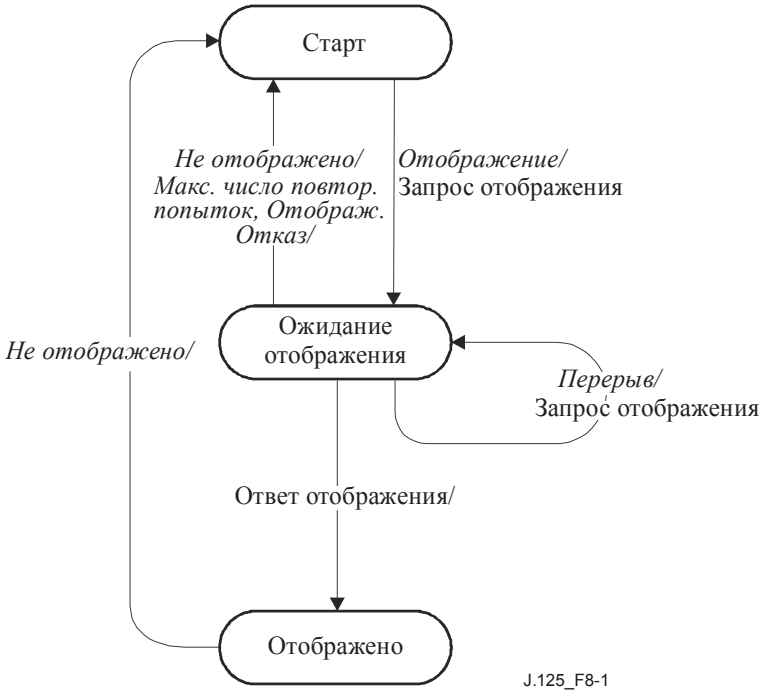


Рисунок 8-1/J.125 – Диаграмма последовательности действий машины состояния отображения SA

Таблица 8-1/J.125 – Матрица переходов состояний динамического SAID

Состояние / ***Событие или полученное сообщение***	**(A) Старт**	**(B) Ожидание отображения**	**(C) Отображено**
(1) *Отобразить*	Ожидание отображения		
(2) *Не отображать*		Старт	Старт
(3) *Ответ на запрос отображения*		Отображено	
(4) *Отказ в отображении*		Старт	
(5) *Время ожидания*		Ожидание отображения	
(6) *Максимум повторений*		Старт	

8.3.1 Состояния

8.3.1.1 Старт (Start)

Начальное состояние конечной машины состояния.

8.3.1.2 Ожидание отображения (Map Wait)

Модем CM уже отправил CMTS запрос на отображение и ждет ответа.

8.3.1.3 Отображено (Mapped)

CM получил ответ об отображении и изучил запрошенное отображение SA.

8.3.2 Сообщения

8.3.2.1 Запрос отображения SA (Map Request)

Запрос отображения SA отправлен модемом CM в CMTS.

8.3.2.2 Ответ отображения SA (Map Reply)

Положительный ответ CMTS на запрос отображения, содержащий запрошенное отображение SA.

8.3.2.3 Отказ отображения SA (Map Reject)

Отрицательный ответ CMTS на запрос CM отображения сигнализирует модему о том, что:

1) CM не авторизован на доступ к потоку трафика, идентифицированного в запросе на отображение; или

2) запрошенный поток трафика не отображен в SA BPI+.

8.3.3 События

8.3.3.1 Отображение (Map)

Инициирует запуск машины состояния отображения SA. Событие отображения связано с событием CM, внешним по отношению к протоколу BPI+.

8.3.3.2 Не отображено (Unmap)

Инициирует завершение машины состояния отображения SA. Неотображенное событие связано с событием CM, внешним по отношению к протоколу BPI+. Использование события Unmap является НЕОБЯЗАТЕЛЬНЫМ.

8.3.3.3 Ответ отображения (Map Reply)

Кабельный модем получает сообщение ответа на отображение SA.

8.3.3.4 Отказ отображения (Map Reject)

Кабельный модем получает сообщение с отказом отображения SA.

8.3.3.5 Время ожидания (Timeout)

Кабельный модем находится в состоянии ожидания ответа на сообщение запроса отображения SA.

8.3.3.6 Максимальное число повторных запросов (Max Retries)

Кабельный модем отправил максимальное число повторных запросов и не получил ответ.

8.3.4 Параметры

Все конфигурации значений параметров определены в файле загрузки параметров TFTP (см. Приложение A).

8.3.4.1 Время ожидания отображения SA (SA Map Wait Timeout)

Период времени между отправкой сообщений с запросами отображения SA и состоянием ожидания SA. См. A.1.1.1.8.

8.3.4.2 Максимальное число попыток запроса отображения SA (SA Map Max Retries)

Максимальное число попыток CM запросить отображение SA перед прекращением запросов.

8.3.5 Действия

Действия, предпринятые в связи с состоянием переходов, перечислены ниже <event/rcvd message> – <state> (<событие/получ. сообщение> – <состояние>):

1-A Start (*Map*) → Map Wait

- отправить запрос на отображение SA;
- установить таймер повтора запроса отображения на время ожидания отображения SA;

- установить счет попыток отображения на 0.

2-B Map Wait (*Unmap*) → Start

- очистить таймер повтора запросов на отображение;
- завершить машину состояния отображения SA.

2-C Mapped (*Unmap*) → Start

- завершить машину состояния отображения SA.

3-B Map Wait (*Map Reply*) → Mapped

- очистить таймер повтора запросов на отображение.

4-B Map Wait (Map Reject) → Start

- очистить таймер повтора запросов на отображения;
- завершить машину состояния отображения SA.

5-B Map Wait (*Timeout*) → Map Wait

- отправить запрос на отображение;
- установить таймер повтора запроса отображения на время ожидания отображения SA;
- увеличить счет повторных запросов на отображение;
- если Map Retry Count > SA Map Max Retries, генерировать событие максимума попыток (Max Retries).

6-B Map Wait (*Max Retries*) → Start

- завершить машину состояния отображения SA.

8.4 Многоадресный трафик IP и динамические SA

В DOCSIS 1.1 [J.112-B] или DOCSIS 2.0 [J.122] определены правила управления трафиком IGMP в CM и CMTS. Эти правила созданы, чтобы управлять потоком многоадресного трафика IP в кабельной сети и на интерфейсе CM/CPE, и заключаются в следующем:

- CMTS только направляет трафик в нисходящем направлении, связанный с многоадресной группой IP, если устройство CPE, присоединенное к одному из клиентов модемов CM CMTS, является членом этой группы; *и*
- CM только направляет через свой интерфейс CPE трафик в нисходящем направлении, связанный с многоадресной группой IP, если присоединенное устройство CPE является членом этой группы.

Интерфейс BPI+, действуя совместно с DOCSIS 1.1 или 2.0 RFI, управляет доступом к потокам многоадресного трафика IP с помощью их шифрования и управления многоадресным материалом распределения и ввода ключей, который требуется для дешифрования потоков.

Система CMTS может отображать многоадресные потоки в нисходящем направлении в любой из трех классов ассоциаций безопасности BPI+: первичный, статический или динамический. Если трафик многоадресной группы IP отображен в первичную SA, то только единственный CM, принадлежащий к этой SA, имеет доступ к этой группе. При отображении в статическую или динамическую SA многие CM имеет доступ к этой группе, хотя CMTS может ограничить статическую или динамическую SA единственным модемом CM.

Если CM DOCSIS 1.1 или 2.0 имеет возможность переслать в нисходящем направлении многоадресную группу IP (в ответ на получение на интерфейс CPE донесения о членстве), то CM ДОЛЖЕН определить, зашифрован ли трафик многоадресной группы IP в нисходящем направлении и связан ли SAID интерфейса с зашифрованным многоадресным потоком в нисходящем направлении. Как только CM связывается с SAID, он может запустить машину состояния TEK для поиска материала распределения и ввода ключей SA.

Модем CM использует механизм отображения SA BPI+ для запроса от своего CMTS отображения SA многоадресной группы IP, к которой он только что присоединился. Событие отображения машины состояния отображения SA запускается с помощью пересылки от RF к CPE многоадресной группы IP

в модем CM (см. B.5.3.1.2 и Приложение L [J.112-B] или 5.3.1.2 и Дополнение V [J.122]). Ответ отображения SA информирует CM о том, что объединенная группа отображена в SA BPI+. Если группа отображена в первичную SA модема CM, то этот CM уже получил материал распределения и ввода ключей. Если группа отображена в статическую или динамическую SA, то CM определяет, находится ли уже в работе машина состояния TEK этой SA; и если нет, то запускает ее.

Машина состояния отображения SA определяет НЕОБЯЗАТЕЛЬНОЕ событие Unmap (не отображено), которое завершает работу машины состояния отображения SA и которое МОЖЕТ быть использовано для указания модему CM более не запрашивать отображенный материал распределения и ввода ключей SA. В случае отображения трафика многоадресного IP в SA, событие Unmap могло бы указать, что CM удалил все фильтры разрешения многоадресных IP, связанных с группами многоадресных IP, отображенных в рассматриваемую SA. Таким образом, машину состояния отображения SA МОЖНО использовать, чтобы отследить необходимость для модема CM сохранять материал распределения и ввода ключей для динамической SA, отображенной в одну или более групп многоадресного протокола IP.

Машины состояния TEK, соответствующие первичным и статическим SAID, останавливают, согласно условиям завершения, описанным в машинах состояния авторизации и TEK.

9 Применение ключей

9.1 CMTS

После окончания модемом CM Регистрации MAC DOCSIS, модем инициирует обмен авторизацией со своей системой CMTS. Первый прием CMTS сообщения запроса на авторизацию от неавторизованных CM инициирует вызов нового ключа авторизация (AK), который CMTS отправляет назад запрашивающему CM в ответ на сообщение авторизации. Этот AK будет оставаться действующим до тех пор, пока не истечет предписанный ему срок жизни, *срок жизни авторизации ключа*, который является параметром конфигурации системы CMTS (см. A.2).

Система CMTS ДОЛЖНА использовать материал распределения и ввода ключей, найденный из ключа авторизации CM для:

- проверки сжатого описания HMAC в запросах ключей, полученное от этого CM;
- шифрования (в режиме EDE двойным ключом по утроенному стандарту DES) TEK в ответах на запрос ключа, которые отправляют этому модему CM (TEK – это податрибут ответа на запрос атрибутов параметров TEK ключа);
- подсчета сжатых описаний HMAC, которые записаны в ответах на запрос ключей, отказов в ключах и недействительности TEK, отправленных этому модему CM.

Система CMTS ДОЛЖНА быть всегда готова отправить CM запрос AK. Система CMTS ДОЛЖНА быть в состоянии поддерживать одновременно до двух действующих AK для каждого клиента CM. Система CMTS имеет два действующих AK во время периода перехода ключа авторизации. Эти два действующие ключа имеют перекрывающиеся сроки жизни.

Период перехода ключа авторизации начинается, когда CMTS получает запрос на авторизацию от CM, и CMTS имеет для этого CM единственный действующий AK. В ответ на этот запрос на авторизацию, CMTS активирует второй AK, который система отправляет обратно запрашивающему CM в ответе на авторизацию. Система CMTS ДОЛЖНА установить действующий срок жизни второго AK с учетом остающегося срока жизни первого AK плюс предписанный *срок жизни ключа авторизации*. Таким образом, второй, "новый" ключ будет оставаться действующим в течение *срока жизни ключа авторизации* после истечения срока жизни первого, "старого" ключа. Период перехода ключа закончится с истечением срока жизни старого ключа. Это показано в верхней половине рисунка 9-1.

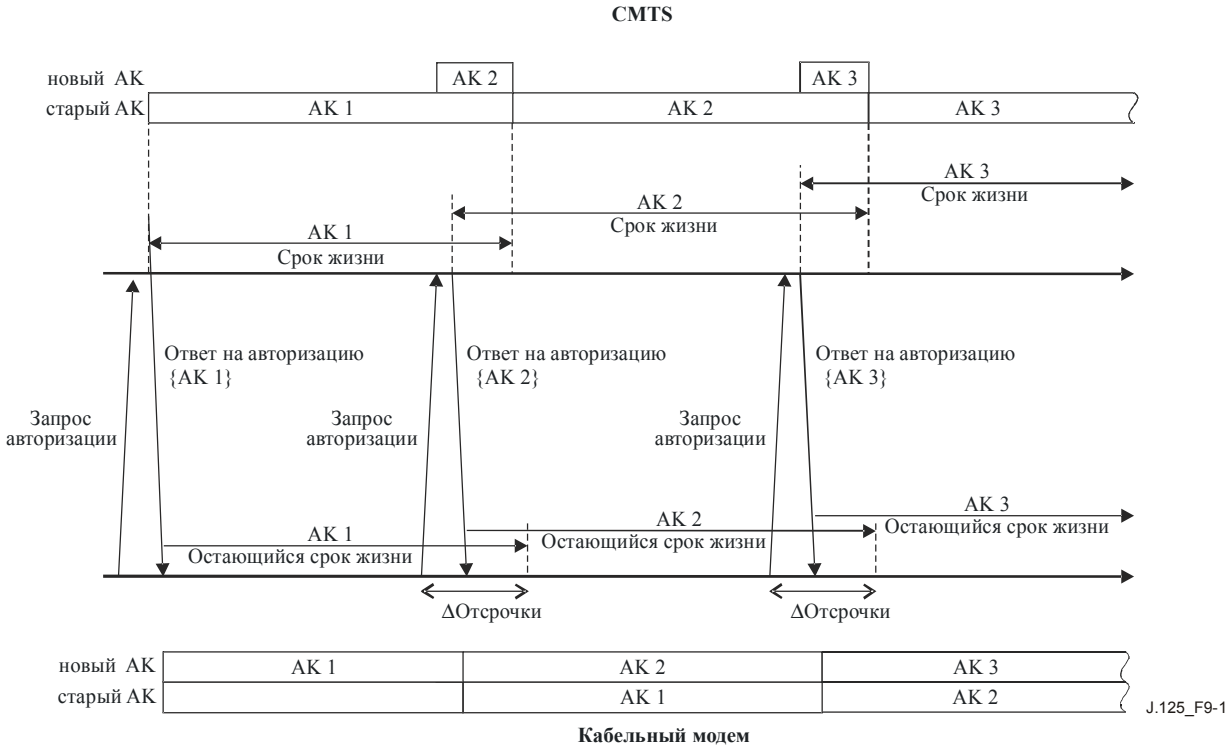


Рисунок 9-1/J.125 – Управление ключом авторизации в CMTS и в CM

Срок жизни ключа авторизации, о котором CMTS сообщает в ответе на авторизацию, ДОЛЖЕН отражать (с точностью, которую допускает применение) остающиеся сроки жизни ключей AK на время отправки сообщения ответа.

Пока CMTS находится в периоде перехода состояния ключа авторизации CM, и, следовательно, удерживает два действующих ключа авторизации для этого CM, система ответит на запрос на авторизацию новым из двух действующих ключей. Как только более старый ключ перестанет действовать, запрос на авторизацию включит активацию нового AK, и начнется новый период перехода ключа.

Если CM не сможет реавторизоваться до истечения срока своего последнего AK, система CMTS будет удерживать недействующие ключи авторизации для CM и будет считать CM *неавторизованным*. Система CMTS ДОЛЖНА удалить из таблиц ключей все ключи TEK, связанные с неавторизованными первичными SA CM.

Система CMTS ДОЛЖНА использовать действующие AK CM для проверки сжатого описания HMAC в запросах ключей, полученных от CM. Если CMTS получает запрос ключа во время переходного периода AK, то сопровождающий номер последовательности ключей AK указывает, что запрос был идентифицирован с новым из двух AK, которые CMTS идентифицирует как *неявное подтверждение* того, что модем CM получил новый из двух действующих ключей AK.

Система CMTS ДОЛЖНА использовать действующий AK при вычислении HMAC в ответе на запрос ключа, отказе на запросы ключа и недействительности TEK, а также при шифровании TEK в ответах ключей. При посылке ответов ключей, отказов в ключе или недействительности ключа TEK в период перехода ключа (т. е. когда доступны оба действующие ключа AK), если новый ключ подтвержден в неявной форме, то система CMTS ДОЛЖНА использовать новый из двух действующих ключей AK. Если новый ключ не был подтвержден в неявной форме, система CMTS ДОЛЖНА использовать старый из двух действующих ключей AK.

Верхняя половина рисунка 9-1 иллюстрирует стратегию CMTS по использованию AK.

Система CMTS ДОЛЖНА поддерживать два набора действующих ключей шифрования трафика (и связанных с ними векторов инициализации CBC) на один SAID. Они соответствуют двум последовательным генерациям материала распределения и ввода ключей и имеют перекрывающиеся сроки жизни. Новый ключ TEK ДОЛЖЕН иметь номер последовательности ключей на единицу

больше (по модулю 16), чем старый TEK. Каждый TEK становится действующим на половине срока жизни своего предшественника и заканчивает функционирование на половине срока жизни последующего ключа. Как только истек срок жизни TEK, ключ TEK становится не действующим и НЕ ДОЛЖЕН более использоваться.

Переходы CMTS между двумя действующими TEK различны в зависимости от того, используют ли TEK в нисходящем направлении или в восходящем направлении трафика. Для каждого из SAID, система CMTS ДОЛЖНА сделать переход между действующими TEK, согласно следующий правилам:

- CMTS ДОЛЖНА использовать старый из двух действующих ключей TEK для шифрования трафика в нисходящем направлении. По истечении срока старого TEK, система CMTS ДОЛЖНА немедленно перейти к использованию нового TEK для шифрования.
- При дешифровании трафика в восходящем направлении период перехода описан таким образом, что он начинается сразу, как только CMTS отправляет новый TEK модему CM в ответ на сообщение запроса ключа. В восходящем направлении период перехода начинается с момента времени, когда CMTS отправляет новый TEK в ответ на сообщение запроса ключа и считает, что срок старого ключа TEK истек. Все же в период перехода CMTS ДОЛЖНА быть в состоянии дешифровать кадры в восходящем направлении, используя либо старый, либо новый ключ TEK.

Система CMTS шифрует с помощью заданного TEK только в течение второй половины срока жизни этого ключа TEK. Система CMTS в состоянии, однако, дешифровать с помощью TEK в течение всего срока жизни TEK.

Поле KEY_SEQ в элементе базовой защиты EH идентифицирует, каким из двух ключей TEK был зашифрован пакет кадра данных в восходящем направлении. Бит TOGGLE в элементе защиты EH, который равен наименее значащему биту поля KEY_SEQ, может использоваться системой CMTS при идентификации шифрования TEK.

В верхней половине рисунка 9-2 проиллюстрировано управление системой CMTS ключами TEK с ассоциациями безопасности BPI+.

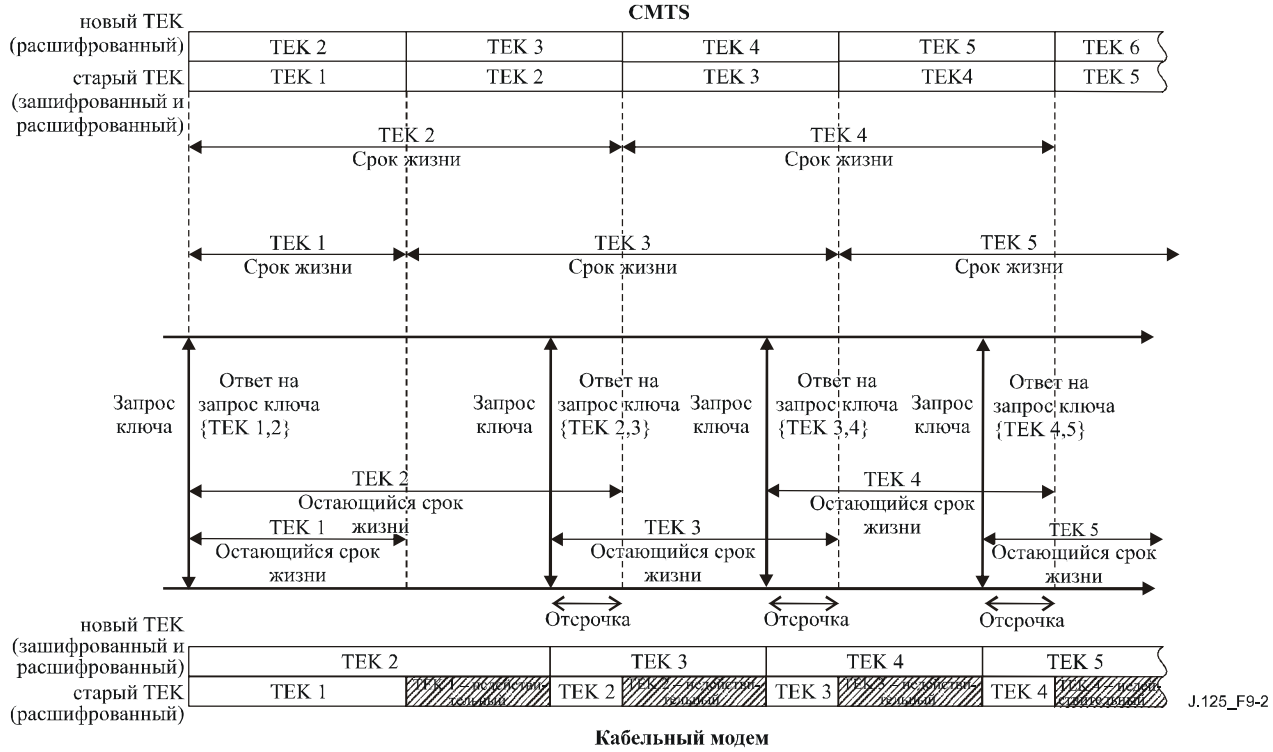


Рисунок 9-2/J.125 – Управление ключами TEK в CMTS и в CM

Система CMTS отвечает за поддержание информации о ключах для первичных и многоадресных SAID указанным выше способом. Протокол управления ключом базовой защиты, описанный в этой Рекомендации, определяет механизм, синхронизирующий обмен информацией о

ключах между CMTS и клиентами модемов CM. Система CMTS отвечает за своевременное обновление ключей для CM. Система CMTS должна переходить к новому ключу шифрования в нисходящем направлении независимо от того, отыскал ли клиент CM копию этого TEK.

Ответ на запросы ключа, отправляемые системой CMTS, содержат параметры TEK (самого TEK, срок жизни ключа, номер последовательности ключей и CBC-IV) для двух действующих ключей TEK. Сроки жизни ключей, о которых CMTS сообщает в ответе на запрос ключей, ДОЛЖЕН отражать (с точностью, которую допускает применение) остающиеся сроки жизни ключей TEK на время отправки сообщения ответа.

9.2 Кабельный модем

Модем CM отвечает за поддержание авторизации с CMTS и поддержание действующего ключа авторизации. Модем CM ДОЛЖЕН быть готов использовать два самые последние ключа AK.

Ключи AK имеют ограниченный срок жизни и ДОЛЖНЫ периодически обновляться. CM обновляет свой ключ авторизации повторным запросом на авторизацию в системе CMTS. Машина состояния авторизации (см. 7.1.2) управляет намеченными запросами на авторизацию для обновления AK.

Машина состояния авторизации CM намечает начало повторной авторизации (реавторизации) с регулируемой продолжительностью времени задержки (*Authorization Grace Time*) до того момента, когда истечет срок действия последнего ключа AK CM. Время задержки авторизации конфигурируют, чтобы обеспечить модем CM повторным периодом, который является достаточно продолжительным, чтобы разрешить системе задержки и обеспечить адекватное время для успешного завершения обмена сообщениями авторизации до истечения срока действия его текущего ключа AK.

ПРИМЕЧАНИЕ. – Система CMTS не требует информации о времени задержки авторизации. Однако CMTS отслеживает сроки жизни авторизации своих ключей и ДОЛЖНА деактивировать ключ, как только истечет его срок действия.

Кабельный модем ДОЛЖЕН использовать более новый из двух последних ключей авторизации при анализе сжатого описания HMAC, которое прилагают к запросу ключей. Модем ДОЛЖЕН быть в состоянии использовать любой из двух последних ключей AK для идентификации запросов ключей, отказов в ключах или недействительности ключей TEK, а также расшифровать ответ на запрос зашифрованного ключа TEK. Модем CM использует сопровождающий AK номер последовательности ключей, чтобы определить, какой из двух ключей AK использовать.

Нижняя половина рисунка 9-2 иллюстрирует поддержку и использование модемом CM авторизации ключей.

CM ДОЛЖЕН быть в состоянии поддерживать два последовательные набора материала распределения и ввода ключей трафика на авторизованном идентификаторе SAID. Во время работы машин состояния TEK модем CM всегда пытается поддерживать два самые последние набора материала распределения и ввода ключей трафика для SAID.

Для каждого из своих авторизованных идентификаторов SAID кабельный модем:

- ДОЛЖЕН использовать более новый из двух TEK, чтобы шифровать вновь полученный трафик в восходящем направлении. Трафик, который уже находится в очереди, МОЖЕТ использовать любой TEK (в неопределенном порядке) в течение короткого периода времени, покрывающего переход от старого к новому ключу.
- ДОЛЖЕН быть в состоянии расшифровывать в нисходящем направлении трафик, зашифрованный любым из ключей TEK.

Поле KEY_SEQ в элементе базовой защиты EH идентифицирует номер последовательности ключей TEK, используемый для шифрования пакетов данных PDU. Бит TOGGLE в элементе защиты EH, который равен наименее значащему биту поля KEY_SEQ, помогает найти различия между двумя последовательными генерациями ключей.

9.3 Идентификация динамических служебных запросов DOCSIS v1.1/2.0

Если программы DOCSIS 1.1 или 2.0 модема CM сконфигурированы для работы BPI+, то спецификация RFI DOCSIS 1.1 [J.112-B] или 2.0 [J.122] требует от CM и CMTS включать сжатое описание HMAC во все дополнительные динамические служебные запросы (DSA-REQ), изменения динамических служебных запросов (DSC-REQ) и удаления динамических служебных запросов (DSD-REQ), которые они отправляют друг другу.

Эти динамические службы сжатого описания HMAC кодируют вместе с сообщениями идентификации ключей BPI+, т. е. сообщения идентификации ключей находят из ключа авторизации BPI+. Модемы CM и системы CMTS ДОЛЖНЫ использовать текущее сообщение

идентификации ключей при генерации и проверке сжатого описания HMAC, которое содержится в динамических служебных запросах.

10 Криптографические методы

Этот раздел определяет криптографические алгоритмы и использует размеры ключа BPI+.

10.1 Шифрование пакетов данных

Базовая защита плюс ДОЛЖНА использовать режим цепочечного блока шифрования (CBC) [FIPS-81] с алгоритмом стандарта США шифрования данных (DES) [FIPS-46-3], чтобы шифровать поле пакета данных RF MAC кадрами пакетов данных PDU, а поля фрагментации полезной нагрузки и фрагментации CRC кадрами фрагментации MAC.

Применения BPI+ в оборудовании DOCSIS 1.1 или 2.0 (с преобладающей конфигурацией ПО и оборудования) ДОЛЖНЫ поддерживать 56-битовый стандарт DES и МОГУТ поддерживать 40-битовый DES.

BPI+ поддерживает в основном 40-битовый DES, чтобы обеспечить взаимодействие с 40-битовым оборудованием DOCSIS 1.0, обновленным для работы с BPI+. 40-битовый стандарт DES идентичен 56-битовому DES, за исключением того, что 16 битов 56-битового ключа DES установлены на известные постоянные значения. Если устройства CM или CMTS работают с необязательным 40-битовым DES, они ДОЛЖНЫ размаскировать (до нуля) шестнадцать крайних левых битов каждого 56-битового ключа DES прежде, чем приступить к операции шифрования/дешифрования.

ПРИМЕЧАНИЕ. – Маскированные биты – это 16 крайние левые биты, которые могли бы быть представлены ПОСЛЕ удаления каждого восьмого бита из 64 битов TEK (т. е. так называемых битов четности). Оборудование DOCSIS 1.1 или 2.0 и 56-битоввое DOCSIS 1.0, функционирующее с BPI+, МОЖЕТ использовать 40-битовый ключ DES, замаскированный в программе.

Режим CBC ДОЛЖЕН быть инициализирован вектором инициализации, который получают вместе с другими материалами ключей в ответе CMTS на запрос ключа. Построение цепью блок за блоком внутри кадра и повторная инициализация на основе кадра делают систему более устойчивой к потенциальной потере кадров.

Остальное завершение обработки блока ДОЛЖНО использоваться для шифрования конечного блока открытого текста, если конечный блок менее 64 битов. При конечном блоке с n битами, где n меньше 64, следующий за последним зашифрованным блоком – это блок, зашифрованный по стандарту DES второй раз с использованием режима ECB, а наименее значащие n битов составляют исключающее ИЛИ с конечными n битами полезной нагрузки для генерации короткого конечного зашифрованного блока. Для дешифрования этого короткого конечного зашифрованного блока приемник DES шифрует предпоследний зашифрованный блок, используя режим ECB и исключающие ИЛИ крайних левых n битов вместе с коротким конечным зашифрованным блоком, чтобы восстановить незашифрованный текст короткого конечного блока. Эта процедура шифрования показана на рисунке 9-4 (стр. 195) в [SCHNEIER].

В специальном случае, когда предполагаемый для шифрования кадр меньше чем 64 бита, вектор инициализации ДОЛЖЕН быть зашифрован по стандарту DES, а крайние левые n битов результирующего открытого текста, соответствующие числу битов полезной нагрузки, ДОЛЖНЫ быть исключающими ИЛИ с n битами полезной нагрузки для генерации короткого конечного зашифрованного блока[6].

---

[6] Этот метод шифрования с короткими полезными нагрузками уязвим для атак: два набора исключающих ИЛИ шифрованного текста, который шифруют указанным выше способом с тем же матриалом распределения и ввода ключей, выдадут на выходе исключающее ИЛИ соответствующего набора открытого текста. Однако, в этом случае кадр пакетных данных PDU, не будет выходом, поскольку все защищенные пользовательские данные кадра будут содержать, по крайней мере 20 байтов заголовка IP. В этом случае фрагментированные кадры, короткий кадр. несущий менее 8 байтов (64 битов) шифрованного текста все же возможны. Однако конечные четыре байта должны быть зашифрованы фрагментированной посылкой CRC, а три или менеебайтов перед фрагментированной CRC должны быть зашифрованы пакетными данными CRC.

10.2 Шифрование TEK

CMTS шифрует значение поля TEK в сообщениях ответа на запрос ключа, которые система посылает клиенту CM. Это поле шифруют, используя режим двух ключевого тройного стандарта DES шифрования–дешифрования–шифрования (EDE) [SCHNEIER]:

кодирование: $C = E_{k1}[D_{k2}[E_{k1}[P]]]$

декодирование: $P = D_{k1}[E_{k2}[D_{k1}[C]]]$

P = незашифрованный текст 64-битового TEK

C = зашифрованный текст 64-битового TEK

k1 = крайние левые 64 бита 128-битового KEK

k2 = крайние правые 64 бита 128-битового KEK

E[ ] = 56-битовый DES ECB (электронная книга кодов) режим шифрования

D[ ] = 56-битовый DES ECB режим дешифрования.

В пункте 10.4 описано, каким образом находят ключи KEK из ключа авторизации.

10.3 Алгоритм сжатого сообщения HMAC

Ключевой хэш, применяемый с атрибутом HMAC-Digest, ДОЛЖЕН использовать метод идентификации сообщения HMAC [RFC2104] по алгоритму хэш SHA-1 [FIPS-180-2].

В восходящем и нисходящем направлении ключи идентификации сообщения находят из ключа авторизации (подробности см. 10.4 ниже).

10.4 Отыскание ключей TEK, KEK и идентификация сообщения

Система CMTS генерирует ключи авторизации, TEK и IV. Для генерации ключей авторизации и TEK ДОЛЖЕН использоваться генератор случайных и псевдослучайных чисел. Генератор случайных и псевдослучайных чисел МОЖНО также использовать для генерации IV. Независимо от способа генерации, ключи IV НЕ ДОЛЖНЫ поддаваться прогнозированию. В [RFC1750] приведена рекомендованная практика для генерации случайных чисел, используемых в криптографических системах.

В [FIPS-81] определены ключи DES в виде 8-октетных (64-битовых) величин, у которых семь наиболее значащих битов (т. е. семь крайних левых битов) каждого октета являются независимыми битами ключа DES, а наименее значащий бит (т. е. крайний правый бит) каждого октета – это бит четности, вычисляемый из семи предшествующих независимых битов и настроенных таким образом, чтобы октет имел проверку на нечётность.

Материал распределения и ввода ключей для двух ключевого тройного алгоритма DES заключается в описании двух различных (единственных) ключей DES.

BPKM не требует проверки на нечетность. Протокол BPKM генерирует и распределяет 8-октетные ключи DES произвольной четности и требует, чтобы применения игнорировали значение наименее значащего бита каждого октета.

Ключ шифрования ключей (KEK) и два ключа идентификации сообщения находят из общего ключа авторизации. Далее определяется, как находят эти ключи:

KEK – Ключ шифрования ключей используют для шифрования ключей шифрования трафика.

HMAC_KEY_U – это ключ идентификации сообщения, который используют для запросов ключей в восходящем направлении.

HMAC_KEY_D – это ключ идентификации сообщения, который используют для запросов ключей, отказов в ключах и сообщениях о недействительности TEK в нисходящем направлении.

SHA(x|y) описывает результат применения функции SHA к объединению строк x и y.

Truncate(x,n) описывает результат усечения x до n крайних левых битов.

```
KEK = Truncate(SHA( K_PAD | AUTH_KEY ), 128)
HMAC_KEY_U = SHA( H_PAD_U | AUTH_KEY )
HMAC_KEY_D = SHA( H_PAD_D | AUTH_KEY )
```

Each _PAD_ – это 512-битовая строка:

K_PAD = 0x53 повторяют 64 раза.

H_PAD_U = 0x5C повторяют 64 раза.

H_PAD_D = 0x3A повторяют 64 раза.

10.5 Открытый ключ шифрования ключа авторизации

Ключи авторизации в сообщениях ответа на авторизацию ДОЛЖНЫ быть открытыми ключами RSA, зашифрованными с использованием открытого ключа кабельного модема. Ключи RSA CM ДОЛЖНЫ использовать F4 (65537 десятичному числу, или эквивалентному 010001 шестнадцатеричному числу) как открытый порядок числа. BPI+ приспосабливает к этому длину модуля из 768 битов (96 октетов) и из 1024 битов (128 октетов). BPI+ использует схему шифрования RSAES-OAEP, определенную для версии 2.0 стандарта PKCS № 1 [RSA3]. Шифрование по RSAES-OAEP требует выбора: хэш-функции, функции генерации маски и параметра кодирования строки. По умолчанию при шифровании ключа авторизации ДОЛЖЕН использоваться выбор, определенный в [RSA3]. Этот выбор по умолчанию состоит из: SHA-1 для хэш-функции, MGF1 с SHA-1 для функции генерации маски и пустой строки для параметра кодирования строки.

Отметим, что базовую защиту [SCTE22-2] используют для схемы шифрования, описанную в версии 1.5 стандарта PKCS № 1 [RSA1]. Это такая же схема, как и RSAES-PKCS1-v1_5 в [RSA3]. Чтобы поддержать обратную совместимость, устройства CM и CMTS ДОЛЖНЫ возвращаться к RSAES-PKCS1-v1_5 [RSA3] для шифрования ключа авторизации при возврате к BPI.

Протокол базовой защиты [SCTE22-2], чья поддержка требуется в модемах CM DOCSIS 1.0, определяет для ключей RSA длину модуля из 768 битов. Чтобы обеспечить обновление программ оборудования CM DOCSIS 1.0 для BPI+, протокол BPI+ ДОЛЖЕН поддерживать 768-битовую, также как и 1024-битовую, длину модулей. Первоначально разработанные модемы CM DOCSIS 1.1 или 2.0 ДОЛЖНЫ использовать ключи RSA, имеющие 1024-битовую длину модуля. Однако обновленные модемы CM от DOCSIS 1.0 до DOCSIS 1.1 или 2.0 МОГУТ использовать ключи RSA, имеющие 768-битовую длину модуля. Для поддержания функциональной совместимости с обновленными модемами v1.0, версии DOCSIS 1.1 или 2.0, использующие BPI+ системы CMTS ДОЛЖНЫ поддерживать 768-битовую и 1024-битовую длину модулей.

10.6 Цифровые подписи

Протокол BPI+ использует алгоритм подписи RSA [RSA3] с SHA-1 [FIPS-186-2] для всех трех типов сертификатов.

Как и для ключей шифрования RSA, BPI+ использует F4 (65537 десятичное, или эквивалентное 010001 шестнадцатеричное число) как открытый порядок числа для операции подписи. Корневой сертификат CA DOCSIS должен использовать длину модуля 2048 битов (256 октетов) для подписи сертификатов CA производителя, которые он выпускает. Сертификаты CA производителей ДОЛЖНЫ использовать длину модуля ключа подписи, по крайней мере, 1024 битов, но не более 2048 битов. Отметим, что корневой сертификат CA DOCSIS должен читаться как CA производителя кабельных модемов J.122.

10.7 Поддерживаемые альтернативные алгоритмы

Текущая спецификация BPI+ требует использовать 56-битовый алгоритм DES для шифрования пакетов данных, двух ключевой тройной алгоритм DES – для шифрования ключей шифрования трафика, 1024-битовый RSA – для шифрования ключей авторизации и от 1024 до 2048-битовых ключей RSA – для подписания сертификатов X.509 BPI+. Выбор длины ключей DES и алгоритмов, будучи подходящим для текущих моделей угроз и возможностей оборудования, может оказаться неподходящим в будущем.

Например, принято, что DES практически уже достиг вершины своей полезности в качестве промышленного стандарта симметричного шифрования. В настоящее время алгоритм NIST считают разработанным и одобренным новым стандартом алгоритма шифрования, в большинстве случаев

принятым как современный стандарт шифрования, или AES. Протокол BPI+ призван поддерживать заданный уровень услуг защиты (с основным уровнем защиты лучшим, чем или равным тому, который обеспечивают выделенные цепи, и условным доступом к услугам транспорта данных RF), а также стратегию гибкого управления ключом (т. е. установкой срока жизни ключей). Основанные на DOCSIS службы провайдеров должны полагаться на DES в течение, по крайней мере, следующих пяти лет. Тем не менее, в будущем кабельные модемы DOCSIS необходимо приспособить к более мощному алгоритму шифрования трафика, возможно AES.

Адаптация нового алгоритма шифрования пакетов данных не должна потребовать реконструкции BPI+. Протокол использует параметры тип/длина/значение, кодирующие атрибуты BPKM, элементы расширенного заголовка MAC и выбор возможностей защиты при обмене авторизацией, что дает гарантию возможности расширения BPI+. В действительности изменения любых криптографических алгоритмов BPI+ или связанных с этим длин ключей не должны влиять на общую структуру и работу этого протокола.

11 Физическая защита ключей в CM и CMTS

BPI+ требует от CM и CMTS поддерживать в устройствах памяти ключи шифрования трафика, а от CM – ключей авторизации. Модем CM ДОЛЖЕН также поддерживать в долговременной, не перезаписываемой памяти пару ключей RSA. Модем CM и система CMTS ДОЛЖНЫ удерживать неавторизованный физический доступ к материалу распределения и ввода ключей.

Уровень физической защиты материала распределения и ввода ключей BPI+, требуемый от CM и CMTS, определен в терминах уровней защиты, описанных в [FIPS-140-2]. В частности, модемы CM и системы CMTS ДОЛЖНЫ удовлетворять требованиям уровня защиты 1 FIPS PUBS 140-2.

Уровень защиты 1 [FIPS-140-2] требует минимальной физической защиты заводских корпусов. Для получения формальных требований читателю СЛЕДУЕТ обратиться к документу FIPS. Однако ниже приведена итоговая сводка этих требований.

По классификации [FIPS-140-2] "физических вариантов конструкций" криптографических модулей, CMTS и внешние модемы CM являются *автономными криптографическими модулями, состоящими из множества чипов.* В [FIPS-140-2] определены следующие требования для уровня защиты 1 автономных криптографических модулей, состоящих из множества чипов:

- Чипы должны быть производственного уровня качества, который должен включать стандартную методику пассивации (т. е. герметичную оболочку вокруг чипа для защиты от окружающих условий и других физических повреждений).
- Компоновка схем в модуле должна выполняться производственным способом компоновки устройств со многими чипами (т. е. на печатной плате интегральных схем, на керамической основе и т. д.).
- Модуль должен быть помещен в металлический или прочный пластиковый корпус промышленного изготовления, который может включать дверцы или съемные крышки.

Внутренний модем CM должен классифицироваться, согласно [FIPS-140-2], как *криптографический модуль со встроенными чипами.* Требования уровня защиты 1 для таких устройств приведены в двух отмеченных выше пунктах.

12 Характеристики и регулирование сертификата X.509 BPI+

BPI+ DOCSIS должен иметь версию 3 [X.509] цифровых сертификатов, для подтверждения обмена ключами между CM CMTS. Документ [X.509] – это общий стандарт, а описанные здесь характеристики сертификата BPI+ дополнительно описывают содержание поля сертификата. Характеристики сертификата также определяют иерархию доверия, описывающую регулирование и правомочность сертификатов BPI+ DOCSIS.

За исключением обратного, отмеченного в следующих разделах, сертификаты BPI+ DOCSIS ДОЛЖНЫ соответствовать стандартам PKIX IETF [RFC3280]. Однако применение сертификатов X.509 DOCSIS более ограничено, чем сертификатов PKIX. Характеристики сертификатов X.509 PKIX IETF имеют целью поддержку независимых применений основанных на сертификатах механизмов распределения ключей в сети Интернет. Характеристики

сертификатов X.509 PKIX ДОЛЖНЫ поддерживать широкий диапазон условий связи, применений и доверительных отношений.

В противоположность этому, использование цифровых сертификатов BPI+ ограничено защитными мерами кабельных операторов от несанкционированного доступа к данным DOCSIS услуг связи с помощью введения условного доступа к ключам шифрования трафика. Защищенные услуги связи делят на три категории:

- услуги передачи данных IP наилучшим образом, с высокой скоростью;
- высококачественные услуги передачи данных CBR (с постоянной скоростью);
- доступ к высококачественным услугам многоадресных групп IP.

Таким образом, хотя BPI+ заимствует многое из характеристик сертификата PKIX IETF, характеристики X.509 BPI+ ограничены значительно в большей степени.

Характеристики сертификата X.509 BPI+ также заимствует многое из стандарта по электронной защите (SET) [SET Book 2]. Многое из общей организации этого раздела и некоторых его подразделов отражает этот стандарт.

12.1 Обзор архитектуры управления сертификата BPI+

Архитектура управления сертификата BPI+ DOCSIS, показанная на рисунке 12-1, состоит из трехуровневой иерархии доверия, поддерживающей три типа сертификатов версии 3 X.509:

- простой с самостоятельной подписью корневой сертификат CA DOCSIS;
- сертификаты CA производителя;
- сертификаты CM.

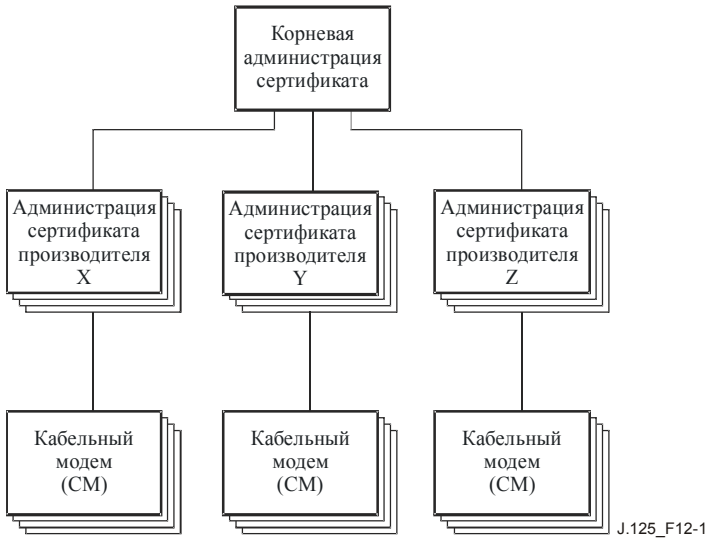


Рисунок 12-1/J.125 – Архитектура управления сертификата DOCSIS

Корневая администрация сертификации служит основным CA для выпуска сертификатов и зависимых сертификатов CA, которые поддерживают производители. Производитель CA выпускает сертификаты для конечных объектов кабельных модемов.

ПРИМЕЧАНИЕ. – Единственный производитель может поддерживать множество CA (например, различный CA для каждого производственного отделения).

В настоящее время, корневая администрации сертификата также служит как корневая CA, для того чтобы издавать сертификат проверки кода (CVC) для загружаемой программы защиты, определенной в Приложении B. Однако с точки зрения защиты нет причин требовать ту же корневую CA, чтобы выпустить как другой сертификат CA производителя, так и CVC. Поэтому в будущем сертификат CVC может быть выпущен другой корневой администрацией сертификата.

Корневой CA должен содержаться под строгим физическим контролем. Этот сертификат должен использоваться редко для выпуска новых сертификатов CA производителя. Организация отвечает за то, чтобы сертификация поддерживала корневой CA. Корневой CA должен генерировать и распространять кабельным операторам список аннулированных сертификатов (CRL), идентифицирующий аннулированные сертификаты производителя. Способ, которым CRL передают кабельным операторам, выходит за рамки спецификации BPI+.

Организация, поддерживающая корневой CA, должна описать протокол выпущенных производителем сертификатов для запрашивающего производителя CA. Однако спецификация этого протокола выходит за рамки спецификации BPI+.

Производители должны быть ответственны за поддержание собственных CA, с помощью которых они будут выпускать сертификаты CM. Один производитель может поддерживать много сертификатов CA производителя. Протоколы, запрашиваемые у производителя сертификатов CA и распространяемые как результирующие сертификаты принимающим кабельным модемом, должны быть внутренними по отношению к этому производителю, и, следовательно, выходят за рамки спецификации BPI+. Производитель CA МОЖЕТ генерировать и распространять кабельным операторам CRL способом; который выходит за рамки спецификации BPI+.

12.2 Формат сертификата

В этом разделе описан формат сертификата X.509 версии 3 и расширения сертификата, которые используют в BPI+. Ниже в таблице 12-1 суммированы основные поля сертификата X.509 версии 3.

Таблица 12-1/J.125 – Основные поля сертификата X.509

Поле X.509 v3	Описание
tbsCertificate.version	Указывает версию сертификата X.509. Всегда устанавливают v3 (значение 2).
tbsCertificate.serialNumber	Однозначное целое число, которое выпускающий CA присваивает сертификату.
tbsCertificate.signature	Идентификатор OID и необязательные параметры, описывающие алгоритм, использованный для подписи сертификата. Это поле ДОЛЖНО содержать тот же идентификатор алгоритма, что и поле signatureAlgorithm ниже.
tbsCertificate.issuer	Отличительное имя администрации CA, выпустившей этот сертификат.
tbsCertificate.validity	Определяет, когда этот сертификат становится действующим и когда его действие прекращается.
tbsCertificate.subject	Отличительное имя идентификации объекта, чей открытый ключ сертифицирован в поле информации открытого ключа субъекта.
tbsCertificate .subjectPublicKeyInfo	Поле содержит материал открытого ключа (открытый ключ и параметры) и идентификатор алгоритма, ключ которого используют.
tbsCertificate .issuerUniqueID	Необязательное поле, которое допускает со временем снова использовать имена выпускающих.
tbsCertificate .subjectUnique ID	Необязательной поле, которое допускает со временем снова использовать имена выпускающих.
tbsCertificate.extensions	Расширение данных.
signatureAlgorithm	Идентификатор OID и необязательные параметры, описывающие алгоритм, использованный для подписи сертификата. Это поле ДОЛЖНО содержать тот же идентификатор алгоритма, что и поле tbsCertificate.
signatureValue	Цифровая подпись, вычисленная по значению ASN.1 DER, закодированному в tbsCertificate.

Все сертификаты и CRL, описанные в этой Рекомендации ДОЛЖНЫ быть подписаны по алгоритму подписи RSA с использованием SHA-1 в качестве однонаправленной функции. Алгоритм подписи RSA, описан в PKCS № 1 RSA1. Алгоритм SHA-1 описан в [FIPS-180-2]. Это только один пример того, как BPI+ ограничивает значения основного поля сертификата X.509. Все эти ограничения описаны ниже:

12.2.1 tbsCertificate.validity.notBefore и tbsCertificate.validity.notAfter

Сертификаты кабельного модема не должны быть возобновляемыми и, таким образом, ДОЛЖНЫ иметь период действия больший, чем эксплуатационный срок жизни кабельного модема. Сертификат производителя CA ДОЛЖЕН быть действительным от даты выпуска на период, описанный в [SCTE23-3] или [SCTE79-2], и возобновлен на период, описанный в [SCTE23-3] или [SCTE79-2]. Корневой сертификат DOCSIS CA ДОЛЖЕН быть действительным от даты, когда начинает действовать корневой CA, на период, описанный в [SCTE23-3] или [SCTE79-2], и возобновлен на период, описанный в [SCTE23-3] или [SCTE79-2].

В этой Рекомендации предполагается, что эксплуатационный срок жизни кабельного модема не превысит двадцати лет. Период действия сертификата кабельного модема ДОЛЖЕН начинаться с даты изготовления устройства. Период действия СЛЕДУЕТ расширить, по крайней мере, до 20 лет после этой даты изготовления.

Периоды действия ДОЛЖНЫ быть закодированы как UTCTime. Значения UTCTime ДОЛЖНЫ быть выражены по среднему времени Гринвича (зулусскому времени) и ДОЛЖНЫ включать секунды (т. е. формат времени: YYMMDDHHMMSSZ) даже в том случае, когда число секунд равно нулю. Поле года (YY) ДОЛЖНО интерпретироваться следующим образом:

- если YY больше или равно 50, год интерпретируют как 19YY;
- если YY меньше 50, год интерпретируют как 20YY.

12.2.2 tbsCertificate.serialNumber

Серийный номер ДОЛЖЕН быть положительным целым числом, приписанным CA к каждому сертификату. Он ДОЛЖЕН быть единственным для каждого сертификата, выпущенного данным CA (т. е. имя выпустившего и серийный номер идентифицируют единственность сертификата). Администрация CA ДОЛЖНА следить, чтобы serialNumber был неотрицательным целым числом. Производителю СЛЕДУЕТ не допускать связи между серийным номером сертификата и серийным номером модема, для которого выпущен этот сертификат.

Указанные выше требования к единственности и серийным номерам могут допускать длинные целые числа. Сертификаты пользователей ДОЛЖНЫ быть в состоянии поддерживать значения serialNumber до 20 октетов. Матрицы отображения CA НЕ ДОЛЖНЫ использовать значения serialNumber более 20 октетов.

ПРИМЕЧАНИЕ. – Чтобы обеспечить обратную совместимость, сертификаты пользователей в системе DOCSIS 1.1 или 2.0 ДОЛЖНЫ быть подготовлены воспринимать сертификаты, серийные номера которых будут отрицательными или нулевыми.

12.2.3 tbsCertificate.signature и signatureAlgorithm

Все сертификаты и CRL, описанные в этой Рекомендации, ДОЛЖНЫ быть подписаны алгоритмом подписи RSA, используя SHA-1 как однонаправленную хэш-функцию. Алгоритм подписи RSA описан в PKCS № 1 [RSA1]; SHA-1 описан в [FIPS-180-2].

Идентификатор OID ASN.1 используют для идентификации "SHA-1 с RSA" по алгоритму подписи:

```
sha-1WithRSAEncription OBJECT IDENTIFIER ::= {
     iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
     pkcs-1(1) 5}
```

Если идентификатор OID sha-1WithRSAEmcription появляется внутри типа идентификатора алгоритма ASN.1, то в этом случае, при наличии tbsCertificate.signature и signatureAlgorithm, параметры компонента этого типа – это тип ASN.1 NULL.

12.2.4 tbsCertificate.issuer и tbsCertificate.subject

Имена X.509 являются ПОСЛЕДОВАТЕЛЬНОСТЯМИ RelativeDistinguishedNames, которые в свою очередь являются установками AttributeTypeAndValue. AttributeTypeAndValue – это ПОСЛЕДОВАТЕЛЬНОСТЬ AttributeType (ИДЕНТИФИКАТОР ОБЪЕКТА) и AttributeValue. Значение атрибута countryName ДОЛЖНО быть двухзначной строкой PrintableString, взятой из ISO 3166. Все прочие Значения AttributeValue ДОЛЖНЫ быть закодированы как строки знаков T.61/TeletexString или PrintableString. Кодирование PrintableString ДОЛЖНО использоваться, если строка знаков содержит только знаки из набора PrintableString set. А именно:

abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
0123456789
'()+,-./:=? and space.

Кодирование T.61/TeletexString ДОЛЖНО использоваться, если строка знаков содержит другие знаки.

Следующие идентификаторы OID необходимы для описания органа, выдающего сертификат, и указанных в сертификате наименований объектов в BPI+:

```
id-at OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) ds(5) 4}
id-at-commonName        OBJECT IDENTIFIER ::= {id-at 3}
id-at-countryName       OBJECT IDENTIFIER ::= {id-at 6}
id-at-localityName              OBJECT IDENTIFIER ::= {id-at 7}
id-at-stateOrProvinceName       OBJECT IDENTIFIER ::= {id-at 8}
id-at-organizationName          OBJECT IDENTIFIER ::= {id-at 10}
id-at-organizationalUnitName    OBJECT IDENTIFIER ::= {id-at 11}
```

Следующие разделы описывают формат поля наименования объекта для каждого типа сертификата BPI+. Поле имени издателя сертификата соответствует полю наименования объекта, выпускающего сертификат. Любой сертификат, который передают в сообщении запроса CM Auth Info или Auth Request, ДОЛЖЕН иметь поле имени, которое соответствует указанному формату. Система CMTS ДОЛЖНА быть в состоянии обработать поля имени сертификата, если поля имени соответствуют указанному формату. Система CMTS МОЖЕТ принять сертификат, у которого поля имени не соответствуют указанному формату.

В общем, сертификаты X.509 поддерживают либеральный свод правил для определения, подходит ли имя издателя сертификата наименованию объекта. Эти правила таковы, что два поля имени могут быть декларированы как соответствующие даже тогда, когда двоичное сравнение этих двух полей имени не указывает на соответствие. В [RFC3280] рекомендуют, чтобы администрации сертификатов ограничили кодирование полей имени таким образом, чтобы его применение могло выявить соответствие или несоответствие, используя простое бинарное сравнение. Протокол BPI+ следует этой Рекомендации. Соответственно, кодированное DER поле tbsCertificate.issuer сертификата BPI+ ДОЛЖНО в точности соответствовать кодированному DER полю tbsCertificate.subject издателя сертификата. Приложение МОЖЕТ сравнить имя издателя с наименованием объекта, выполнив бинарное сравнение кодированных DER полей tbsCertificate.issuer и tbsCertificate.subject.

12.2.4.1 Корневой сертификат DOCSIS

countryName=US

organizationName=Спецификация интерфейса службы передачи данных по кабелю

organizationalUnitName=Кабельные модемы

commonName=Администрация корневого сертификата кабельного модема DOCSIS

Атрибуты countryName, organizationName, organizationalUnitName и commonName ДОЛЖНЫ быть включены и ДОЛЖНЫ иметь указанные значения. Прочие атрибуты не допускаются и НЕ ДОЛЖНЫ быть включены.

12.2.4.2 Сертификат производителя DOCSIS

countryName=<Страна-производитель>
[stateOrProvinceName=<страна/область>]
[localityName=<Город>]

organizationName=<Наименование компании>

organizationalUnitName=DOCSIS

[organizationalUnitName=<Местоположение производства>]

commonName=<Наименование компании> [<Идентификатор серии>] Администрация корневого сертификата кабельного модема [<Идентификатор серии>]

Атрибуты countryName, organizationName и commonName ДОЛЖНЫ быть включены и ДОЛЖНЫ иметь указанные значения..

Атрибут commonName МОЖЕТ содержать идентификатор серии (например, 1, 2, ONE, TWO, A, B, I, II, и т. д.) для идентификации различных производителей CA, размещенных теми же производителями с тем же наименованием компании.

Атрибут organizationalUnitName со значением "DOCSIS" ДОЛЖЕН быть включен.

Атрибут organizationalUnitName, представляющий расположение производства, СЛЕДУЕТ включить. При включении этот атрибут ДОЛЖЕН предшествовать атрибуту organizationalUnitName, имеющему значение "DOCSIS."

Атрибуты stateOrProvinceName и localityName МОГУТ быть включены.

Прочие атрибуты не допускаются и НЕ ДОЛЖНЫ быть включены.

12.2.4.3 Сертификат кабельного модема

countryName=<Страна-производитель>

organizationName=<Наименование компании>

organizationalUnitName=<Местоположение производства>

commonName=<Серийный номер>

commonName=<MAC адрес>

Чтобы различить два атрибута commonNames, атрибут commonName, представляющий "Серийный номер", ДОЛЖЕН предшествовать атрибуту commonName, представляющему "MAC адрес". Использование поля "Серийный номер" не рекомендуется. Если же это поле используют, то серийный номер ДОЛЖЕН быть однозначным идентификатором кабельного модема, но МОЖЕТ отличаться от серийного номера, закодированного в атрибутах BPKM. MAC адрес в сертификате CM ДОЛЖЕН быть таким же, как MAC адрес в атрибутах BPKM.

Знаки, используемые при представлении в PrintableString серийных номеров модемов, ДОЛЖНЫ быть ограничены следующим подмножеством знаков:

- A-Z (0x41-0x5A)
- a-z (0x61-0x7A)
- 0-9 (0x30-0x39)
- "–" (0x2D).

MAC Адрес выражают как шесть пар шестнадцатеричных цифр, разделенных двоеточиями (:), например, "00:60:21:A5:0A:23". Знаки Alpha HEX (A-F) ДОЛЖНЫ быть выражены заглавными буквами.

Атрибуту organizationalUnitName в сертификате кабельного модема, который описывает место производства модема, СЛЕДУЕТ быть таким же, как organizationalUnitName в атрибуте имени издателя, где описывают расположение производства.

Атрибуты countryName, organizationName, organizationalUnitName и commonName (MAC Адрес) ДОЛЖНЫ быть включены. Атрибут commonName (Серийный номер) МОЖЕТ быть включен. Прочие атрибуты не допускаются и НЕ ДОЛЖНЫ быть включены.

12.2.5 tbsCertificate.subjectPublicKeyInfo

Поле tbsCertificate.subjectPublicKeyInfo содержит открытый ключ и идентификатор алгоритма открытого ключа. Открытый ключ RSA в сертификате модема СМ ДОЛЖЕН быть таким же, как открытый ключ RSA в атрибутах BPKM.

Поле tbsCertificate.subjectPublicKeyInfo.algorithm находится в структуре идентификатора алгоритма. Алгоритм AlgorithmIdentifier ДОЛЖЕН быть зашифрован RSA и идентифицирован следующими идентификаторами OID:

```
pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) 1}

rsaEncription OBJECT IDENTIFIER ::= { pkcs-1 1}
```

Поле параметров AlgorithmIdentifier ДОЛЖНО иметь тип NULL ASN.1.

Открытый ключ RSA должен быть закодирован с использованием типа RSAPublicKey ASN.1:

```
RSAPublicKey ::= SEQUENCE {
     modulus            INTEGER, -- n
     publicExponent     INTEGER, -- e -- },
```

где модуль – это модуль n, а publicExponent – обычная экспонента e. Кодированное алгоритмом DER RSAPublicKey – это значение BIT STRING tbsCertificate.subjectPublicKeyInfo.subjectPublicKey.

12.2.6 tbsCertificate.issuerUniqueID и tbsCertificate.subjectUniqueID

Поля issuerUniqueID и subjectUniqueID ДОЛЖНЫ быть опущены для всех трех типов сертификатов BPI+.

12.2.7 tbsCertificate.extensions

Сертификаты кабельных модемов и сертификаты CA производителей DOCSIS не требуют включения никаких расширений. Это справедливо даже для расширений по [RFC3280]. Сертификаты кабельных модемов и сертификаты CA производителей DOCSIS могут включать расширения, как это описано соответственно в 12.2.7.1 и в 12.2.7.2. В подпункте 12.2.7.3 определены требования к расширениям корневых сертификатов CA. Расширения, включенные в сертификаты BPI+, ДОЛЖНЫ соответствовать [RFC3280].

12.2.7.1 Сертификаты кабельных модемов

Сертификаты кабельных модемов МОГУТ содержать некритичные расширения, но НЕ ДОЛЖНЫ содержать критичные расширения. Если присутствует расширение KeyUsage, то биты digitalSignature и keyEncipherment ДОЛЖНЫ быть включены, биты keyCertSign и cRLSign ДОЛЖНЫ быть выключены, а все прочие биты СЛЕДУЕТ выключить. Расширение Basic Constraints МОЖЕТ появиться в сертификатах кабельных модемов как некритичное расширение.

12.2.7.2 Сертификаты CA производителей DOCSIS

Сертификаты CA производителей DOCSIS МОГУТ содержать расширение Basic Constraints и/или расширение KeyUsage. Если такие расширения включены, то они МОГУТ появиться как критичные расширения или некритичные расширения.

Сертификаты CA производителей DOCSIS МОГУТ содержать некритичные расширения, но они НЕ ДОЛЖНЫ содержать критичные расширения иные, чем, возможно, расширения Basic Constraints и KeyUsage.

Если в сертификате CA производителя DOCSIS присутствует расширение KeyUsage, бит keyCertSign ДОЛЖЕН быть включен, бит cRLSign МОЖЕТ быть включен, а все прочие биты СЛЕДУЕТ выключить.

Если присутствует расширение Basic Constraints, сертификат CA ДОЛЖЕН быть установлен на TRUE, а значение pathLenConstraint ДОЛЖНО быть установлено на 0.

12.2.7.3 Корневой сертификат CA DOCSIS

Корневой сертификат CA DOCSIS ДОЛЖЕН содержать расширение Basic Constraints и расширение KeyUsage как критичные.

Корневой сертификат CA DOCSIS МОЖЕТ содержать некритичные расширения. но НЕ ДОЛЖЕН содержать критичные расширения иные, чем Basic Constraints и KeyUsage.

Для расширения KeyUsage, бит keyCertSign ДОЛЖЕН быть включен, бит cRLSign МОЖЕТ быть включен, а все прочие биты СЛЕДУЕТ выключить.

Для расширения Basic Constraints, CA ДОЛЖНО быть установлено на TRUE, а pathLenConstraint ДОЛЖНО быть установлено на 1.

12.2.8 Атрибут signatureValue

Во всех трех типах сертификатов BPI+ атрибут signatureValue содержит подписи RSA (с SHA-1), вычисленные из кодированного DER ASN.1 значения tbsCertificate. Кодированное DER ASN.1 значение tbsCertificate используют как вход функции подписи RSA. Результирующее значение подписи – это кодированная ASN.1 строка BIT STRING, включенная в поле сертификата signatureValue.

12.3 Хранение и управление сертификатами кабельного модема в CM

Наименование производителя, выпускающего сертификаты модемов CM, ДОЛЖНО сохраняться в долговременной (только для чтения) памяти CM. Модемы CM, которые имеют инсталлированные на заводе частную/открытую пару ключей RSA, ДОЛЖНЫ также иметь инсталлированные на заводе сертификаты CM. Модемы CM, которые полагаются на внутренние алгоритмы генерации пары ключей RSA, ДОЛЖНЫ поддерживать механизм инсталлирования сертификата производителя-издателя CM следующим ключом генерации.

Корневой открытый ключ CA для проверки CVC, который CM использует, чтобы проверить код проверки сертификата (CVC) для загружаемой программы защиты, описанной в Приложении B, ДОЛЖЕН быть помещен в не разрушаемую память CM. Хотя в настоящее время корневая администрация CA DOCSIS выпускает для кабельного модема последовательность кодов CVC, в будущем другая корневая администрация CA может выпускать CVC. Поэтому CM НЕ ДОЛЖЕН использовать корневой открытый ключ CA для проверки кода CVC, встроенного в не разрушаемую память CM, чтобы проверить последовательность сертификатов кабельного модема.

Сертификат CA производителя, который подписывает сертификат, ДОЛЖЕН храниться в не разрушаемой памяти кабельного модема. Кабельный модем ДОЛЖЕН быть в состоянии обновлять и заменять сертификат CA производителя с помощью файла загрузки кода DOCSIS (см. Приложение B). Сертификат CA производителя МОЖЕТ быть встроен в программное обеспечение CM.

В тех случаях, когда сертификат CA производителя встроен в ПО CM, а производитель выпускает сертификаты CM с многими сертификатами CA, память CM ДОЛЖНА включать ВСЕ сертификаты CA производителя. Специальный сертификат CA производителя, инсталлированный в CM (т. е. объявленный в сообщении с информацией об идентификации и возвращенный объектом MIB), должен идентифицировать издателя этого сертификата модема.

12.4 Обработка и управление сертификатами в CMTS

Система управления BPKM использует цифровые сертификаты, чтобы позволить CMTS проверить связь между идентичностью CM (закодированной в наименованиях объектов цифрового сертификата X.509) и его открытым ключом. Система CMTS выполняет это, проверяя путь или цепочку сертификатов CM. Обычно этот путь состоит из трех связанных сертификатов: начиная с сертификата CM, этот путь ведет к сертификату CA производителя, который выпустил

сертификат CM, и заканчивается корневым подписанным сертификатом CA DOCSIS (рисунок 12-2). Цепь проверки означает проверку подписи производителя сертификата CA открытым ключом CA корневого оборудования DOCSIS и далее проверку подписи сертификата CM открытым ключом производителя CA.

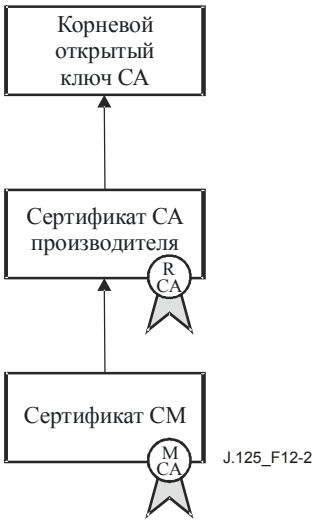


Рисунок 12-2/J.125 – Цепь сертификации CM

Протокол BPI+ требует, чтобы системы CMTS поддерживали административное управление, которое позволит оператору заменять цепь проверки сертификации определением доверия или недоверия к CA производителя или к сертификату CM. Подробное описание этих административных проверок по управлению сертификатами в CMTS дано в объединенном документе OSS BPI+ [DOCSIS8]. В этом разделе определена модель управления с использованием этих проверок, а также обработка, которую производит CMTS, чтобы получить доступ для проверки достоверности сертификата CM и тем самым проверить связь между идентичностью CM и его открытым ключом.

12.4.1 Модель управления сертификатами CMTS

Система CMTS содержит копии корневого CA, сертификаты CA производителя и кабельного модема, которые система получает либо при инициализации, либо с помощью сообщений BPKM. Каждый сертификат, который изучает система CMTS, ДОЛЖЕН маркироваться одним из четырех состояний: "доверия", "недоверия", "связанный" или "корневой". Только корневой сертификат CA DOCSIS (подписанный лично сертификат, который содержит открытый ключ доверия корневого CA DOCSIS) ДОЛЖЕН маркироваться как корневой. Однако CMTS МОЖЕТ поддерживать много корневых сертификатов CA. Корневые сертификаты ДОЛЖНЫ быть заготовлены в CMTS и система CMTS ДОЛЖНА поддерживать функцию, которая показывает собственно корневые сертификаты и/или их отпечатки с тем, чтобы оператор мог проверить корневые сертификаты.

Система CMTS изучает сертификаты CA производителя либо при инициализации интерфейса CMTS, либо из принятых и обработанных сообщений клиентов CM с информацией об идентификации. Независимо от того, как CMTS получает сертификаты CA производителя, система CMTS ДОЛЖНА маркировать их либо как доверия, недоверия, либо как связанный. Если сертификат CA производителя *не подписан лично*, CMTS маркирует этот сертификат как связанный. Система CMTS, однако, ДОЛЖНА поддерживать административное управление, которое позволит оператору отменить маркировку "связанный" и отметить данный сертификат CA производителя как "доверия" или "недоверия".

Если сертификат CA производителя *подписан лично*, CMTS маркирует этот сертификат как либо "доверие", либо "недоверие", согласно административной политике контроля CMTS. Подписанный лично сертификат CA производителя, чья подпись не может быть проверена, ДОЛЖЕН маркироваться как "недоверие". Система CMTS, доверяющая личной подписи сертификатов CA производителя ДОЛЖНА иметь перестраиваемую конфигурацию. Доверие личной подписи

сертификатов CA производителей по умолчанию НЕ РЕКОМЕНДУЕТСЯ при коммерческой эксплуатации систем. Преимущественно доверие по умолчанию могло бы использоваться для поддержания сертификации и других режимов испытаний. Система CMTS ДОЛЖНА маркировать сертификат CM как "связанный", пока не последует отмены со стороны административного управления CMTS.

Система CMTS содержит копии сертификатов кабельных модемов в запросах на авторизацию, которые система получает от клиентов CM. Сертификаты кабельных модемов ДОЛЖНЫ быть выпущены Производителем CA. Таким образом, до отмены административным управлением CMTS, система CMTS будет маркировать сертификаты CM как "связанные". Оператор может как часть процесса инициализации модема, определить, был ли данный сертификат CM маркирован как "доверие" либо "недоверие".

12.4.2 Проверка сертификата

Система CMTS проверяет пути сертификации CA производителя и сертификатов CM, используя следующие критерии.

ПРИМЕЧАНИЕ. – Критерии являются итеративными, и система CMTS ДОЛЖНА проверить путь сертификации связанного сертификата CA производителя, прежде чем эта система сможет проверить путь сертификации сертификата CM, выпущенного этой CA производителя.

Система CMTS ДОЛЖНА разделить на категории CA производителя и сертификаты кабельного модема как действительный или недействительный, если пути их сертификации соответственно действительные или недействительные. Сертификаты доверия ДОЛЖНЫ быть действительными. Это справедливо, если текущее время действия не противоречит периоду "доверия" сертификата. Сертификаты "недоверия" ДОЛЖНЫ быть недействительными.

"Связанный" сертификат является действительным, если:

1) этот сертификат связан с сертификатом корневым, доверия или действительным;
2) подпись сертификата может быть проверена открытым ключом выпускающего;
3) текущее время попадает на период действия каждого связанного или корневого сертификата внутри цепи сертификатов (BPI+ не требует вложения периодов действия, т. е. полному периоду действительности сертификата не требуется попадать в период действия выпущенного сертификата);
4) сертификат не находится в списке "горячих" (рискованных) сертификатов CA производителей и сертификатов CM (см. 12.4.4);
5) в случае сертификата CM, MAC адрес CM, закодированный в поле tbsCertificate.subject, и открытый ключ RSA, закодированный в поле tbsCertificate.subjectPublicKeyInfo, совпадают с MAC адресом CM и открытым ключом RSA, закодированными в атрибутах BPKM запроса на авторизацию;
6) в случае сертификата CM, если присутствует расширение KeyUsage, то биты digitalSignature и/или keyAgreement включены, бит keyEncipherment включен, а биты keyCertSign и cRLSign выключены. В случае сертификата CA производителя, если присутствует расширение KeyUsage, то бит keyCertSign включен.

Будет ли игнорироваться критерий 3 – это ДОЛЖНО быть прерогативой управляющей администрации.

Если проверка периода действительности показывает ENABLED. а макрокоманда "время дня" еще не принята системой CMTS, то (недолговременное) сообщение отказа в авторизации ДОЛЖНО быть возвращено в ответ на запрос метода авторизации BPI+.

Если "связанный" сертификат не удовлетворяет ни одному из вышеприведенных критериев действительности, система CMTS ДОЛЖНА идентифицировать его как недействительный.

12.4.3 Отпечатки сертификата

Отпечатки являются средством сопротивления столкновению однонаправленных хэш-функций (например, SHA-1) сертификатов. Они обеспечивают компактный способ идентификации сертификатов. Система CMTS МОЖЕТ удерживать отпечатки сертификатов CM и CA Производителя, которые система держит или проверила. Используя отпечатки, система CMTS может помещать в кэш-память результаты операции проверки: соответствия отпечатка вновь предложенного сертификата с помещенным в кэш-память отпечатком, и может быстро определить действительность предложенного сертификата.

12.4.4 Списки "горячих" сертификатов CM и CA производителя

При проверке цепи сертификатов системе CMTS не требуется контролировать статус аннулирования сертификата (т. е. проверять присутствие сертификата в обновленном списке CRL). Однако CMTS ДОЛЖНА быть в состоянии поддерживать *горячие списки* известных сертификатов CA производителя и CM, которые находятся в категории "недоверия". Сертификаты в этих *горячих списках* могут включать сертификаты, аннулированные их издателями. Однако они могут также включать действующие сертификаты, которые кабельный оператор, работающий с CMTS, отметил "недоверием".

Определение процедур и протоколов для поддержания в системе CMTS горячих списков сертификатов CA производителей и сертификатов CM выходит за рамки Рекомендации BPI+.

Приложение A

Расширения файла конфигурации TFTP

Все значения параметров конфигурации базовой защиты CM определены в конфигурации файл TFTP, который загружается модемом CM во время инициализации RF MAC. Установки полей конфигурации базовой защиты включены в расчеты MIC CM и MIC CMTS, а также в запросы регистрации CM. Ссылки [J.112-B] на порядок, в котором устанавливают поля конфигурации базовой защиты, включены в сжатом виде в MD5 MIC CMTS.

A.1 Кодирование

Параметры кодирования тип/длина/значение ДОЛЖНЫ использоваться для любой установки конфигурации базовой защиты, включенных в файл конфигурации. Установки конфигурации базовой защиты в запросах на регистрацию CM RF MAC ДОЛЖНЫ быть такими же, как и те, которые включены в файл конфигурации. Все величины из многих октетов располагаются в сетевом порядке байтов, *т. е.* октет, содержащий наиболее значащие биты, поступает в линию первым.

A.1.1 Установка конфигурации базовой защиты

Установка комбинации защиты персональной информации RFI 1.1 или 2.0 по ([J.112-B] пункт B.C.1.1.16) или по [J.122], а также установка возможностей поддержки модемом защиты по ([J.112-B] пункт B.C.1.3.1.6) или по [J.122] контролируют, возможна или невозможна в модеме базовая защита плюс. Если оператор предполагает обеспечить работу CM в режиме BPI+, используя по умолчанию конфигурацию параметров BPI, описанную в таблице A.1, то соответствующие дополнительные установки файла конфигурации базовой защиты МОГУТ быть опущены. Если файл конфигурации не содержит все необходимые параметры BPI+, модем CM ДОЛЖЕН использовать значения по умолчанию, описанные в таблице A.1 для недостающих параметров. С другой стороны, если оператор предполагает обеспечить работу CM в режиме BPI+, используя параметры конфигурации BPI, отличные от значений по умолчанию в таблице A.1, то ДОЛЖНЫ быть представлены дополнительные установки конфигурации базовой защиты. Установки конфигурации базовой защиты МОГУТ быть представлены, если базовая защита плюс отключена. Отдельный параметр включения защиты позволит оператору отключить или вновь включить базовую защиту, периодически переключая единственный параметр конфигурации, что не требует удаления и повторного включения дополнительной установки параметров конфигурации базовой защиты.

Это поле определяет параметры, связанные с работой базовой защиты. Поле состоит из ряда инкапсулированных полей тип/длина/значение. Описанные типы полей являются единственными действующими в инкапсулированной строке конфигурации базовой защиты.

тип	длина	значение
BP_CFG	n	

B [J.112-B] или в [J.122] определено специальное значение BP_CFG.

A.1.1.1 Кодирование внутренней базовой защиты

A.1.1.1.1 Время ожидания авторизации

Значение этого поля определяет интервал (в секундах) повторных передач сообщений запросов на авторизацию из состояния ожидания авторизации.

подтип	длина	значение
1	4	

Действующий диапазон: 1-30

A.1.1.1.2 Время ожидания повторной авторизации

Значение этого поля определяет интервал (в секундах) повторных передач сообщений запросов на авторизацию из состояния ожидания авторизации.

подтип	длина	значение
2	4	

Действующий диапазон: 1-30

A.1.1.1.3 Время задержки авторизации

Значение этого поля определяет период задержки (в секундах) повторной авторизации.

подтип	длина	значение
3	4	

Действующий диапазон: 1-6 047 999

A.1.1.1.4 Эксплуатационное время ожидания

Значение этого поля определяет интервал повторной передачи (в секундах) запросов ключей из состояния ожидания операции.

подтип	длина	значение
4	4	

Действующий диапазон: 1-10

A.1.1.1.5 Время ожидания смены ключа

Значение этого поля определяет интервал повторной передачи (в секундах) запросов ключей из состояния ожидания смены ключей.

подтип	длина	значение
5	4	

Действующий диапазон: 1-10

A.1.1.1.6 Время задержки ключа TEK

Значение этого поля определяет период задержки (в секундах) смены ключа TEK.

подтип	длина	значение
6	4	

Действующий диапазон: 1-302399

A.1.1.1.7 Время ожидания отказа в авторизации

Значение этого поля определяет, как долго CM находится в состоянии ожидания (в секундах) отказа на авторизацию после получения отказа на авторизацию.

подтип	длина	значение
7	4	

Действующий диапазон: 1-600

A.1.1.1.8 Время ожидания отображения SA

Значение этого поля определяет интервал повторной передачи (в секундах), от состояния запросов на отображение до состояния ожидания отображения SA.

подтип	длина	значение
8	4	

Действующий диапазон: 1-10

A.1.1.1.9 Максимальное число попыток отображения SA

Значение этого поля определяет максимально допустимое число попыток запросов на отображения.

подтип	длина	значение
9	4	

Действующий диапазон: 0-10

A.2 Рекомендации по параметрам

Ниже приведены рекомендуемые диапазоны и различные значения конфигураций базовой защиты, а также эксплуатационные параметры. Эти диапазоны и значения по умолчанию могут меняться, поскольку провайдеры услуг приобрели эксплуатационный опыт по применению базовой защиты.

Таблица A.1/J.125 – Рекомендуемые эксплуатационные диапазоны для параметров конфигурации BPI

Система	Наименование	Описание	Миним. значение	Значение по умолчанию	Максим. значение
CMTS	Срок жизни авторизации	Срок жизни в секундах присвоения системой CMTS нового ключа авторизации	1 день (86 400 с)	7 дней (604 800 с)	70 дней (6 048 000 с)
CMTS	Срок жизни TEK	Срок жизни в секундах присвоен. системой CMTS новому ключу TEK	30 мин. (1 800 с)	12 часов (43 200 с)	7 дней (604 800 с)
CM	Время ожидания авторизации	Интервал повторн. передачи запроса на авториз. из состояния ожидания авториз.	2 с	10 с	30 с
CM	Время ожидания повторной авторизации	Интервал повторн. передачи запроса на авториз. из состояние ожидания повторн. запроса	2 с	10 с	30 с
CM	Время задержки авторизации	Время от срока окончания авторизации до начала запроса CM новой авторизации	5 мин. (300 с)	10 мин. (600 с)	35 дней (3 024 000 с)
CM	Эксплуатационное время ожидания	Интервал передачи запр. ключа из состояния ожидания экспл.	1 с	с	10 с

Таблица A.1/J.125 – Рекомендуемые эксплуатационные диапазоны для параметров конфигурации BPI

Система	Наименование	Описание	Миним. значение	Значение по умолчанию	Максим. значение
CM	Время ожидания смены ключа	Интервал передачи запр. ключа из состояния ожидания смены ключа	1 с	10 с	10 с
CM	Время задержки ключа	Время от срока окончания нового TEK до начала смены ключа CM	5 мин. (300 с)	1 час (3 600 с)	3,5 дня (302 399 с)
CM	Ожидание отказа авторизации	Задержка между повторным запросом на автор. после получения отказа в авторизации	10 с	60 с	10 мин. (600 с)
CM	Время ожидания отображения SA	Интервал между запрос. отображения и состоянием ожидания отображения	1 с	1 с	10 с
CM	Максимальное число попыток отображения SA	Максимальное число попыток CM запросов отображения SA перед прекращением запросов	0	4	10

Действующий диапазон (по отношению к рекомендуемому эксплуатационному) для сроков жизни авторизации и TEK:

- Действующий диапазон срока жизни авторизации: 1-6 048 000 секунд.
- Действующий диапазон срока жизни TEK: 1-604 800 секунд.

Действующие диапазоны описаны для каждых параметров конфигурации BPI, расположенных ниже рекомендуемых эксплуатационных диапазонов. Для целей протокольных испытаний полезно запустить протокол BPI с таймером значений много ниже конца рекомендуемых эксплуатационных диапазонов. Более короткие значения таймера "ускорят" часы, что приведет к более быстрой смене событий машины состояния протокола BPI, чем при "эксплуатационной" конфигурации. Хотя нет смысла применять BPI в таком эффективном ритме работы, использование этого протокола СЛЕДУЕТ проводить при сокращенных значениях таймера. В таблице A.2 приведен список сокращенных значений параметров, которые желательно использовать в протоколе соответствия и при сертификационных испытаниях.

Таблица A.2/J.125 – Сокращенные значения параметров BPI для испытаний по протоколу

Срок жизни авторизации	5 мин. (300 с)
Срок жизни TEK	3 мин. (180 с)
Время задержки авторизации	1 мин. (60 с)
Время задержки TEK	1 мин. (60 с)

Время задержки TEK ДОЛЖНО быть меньше половины срока жизни TEK.

Приложение B

Проверка загруженного эксплуатационного программного обеспечения (ПО)

B.1 Введение

Система DOCSIS поддерживает удаленную загрузку кода для сетевых кабельных модемов. Источник и сохранность этого загруженного кода важна для всей работы и защиты системы DOCSIS.

Модуль загрузки ПО является притягательной мишенью для злоумышленников. Если злоумышленник будет в состоянии произвести масштабную атаку на модуль загрузки ПО, то потенциально он может инсталлировать код, чтобы вывести из строя все СМ в зоне или серьезно нарушить обслуживание. Чтобы разрушить эти атаки, злоумышленник ДОЛЖЕН быть принужден преодолевать несколько барьеров защиты.

B.2 Обзор

Требования, описанные в этом разделе, относятся к целям первичной защиты – процессу загрузки кода:

- СМ следует иметь средства аутентифицировать любой источник загрузки кода как известный и заслуживающий доверия.
- СМ следует иметь средства проверить, что загруженный код не изменялся от оригинального состояния, в котором он был доставлен от заслуживающего доверия источника.
- Этот процесс должен упростить требования к обработке файла кода оператором кабельной сети и обеспечить оператору кабельной сети механизмы для обновления и понижения версии кода кабельный модемов в сети.
- Этот процесс должен также разрешить оператору кабельной сети проводить собственную политику и управлять из первых рук тем, что касается:
  a) какие файлы кодов должны быть приняты кабельными модемами в их сетевой зоне; и
  b) управление защитой, определяющее защиту процессов в их сети.
- Кабельные модемы должны быть в состоянии свободно перемещаться между системами, контролируемыми различными организациями операторов кабельной сети.
- Корневой открытый ключ CA (необязательное): обновленный корневой открытый ключ CA, должен заменить корневой открытый ключ CA, хранимый в данный момент в СМ.
- Сертификаты производителя (необязательное): один или более сертификатов производителя, совместимых с X.509, должны заменять сертификаты производителя, хранимые в данный момент в СМ.

В этой Рекомендации область применения ограничена требованиями системы первичной защиты, но предполагается, что в некоторых случаях желательна дополнительная защита. Опасения индивидуальных операторов кабельной сети или производителей кабельных модемов могут привести к созданию дополнительной защиты, касающейся распределения и инсталляции кода в кабельный модем или другой элемент сети DOCSIS. Данная Рекомендация не ограничивает использование дополнительной защиты в тех случаях, когда эта защита не вступает в конфликт с намерениями и руководствами этой Рекомендации.

Существует много уровней защиты, которые требуются для успешной защиты и проверки загрузки кода.

- Производитель кода СМ всегда прикладывает к файлу кода цифровую подпись. Эта подпись подтверждается последовательностью сертификатов, вплоть до корневого DOCSIS. Подпись производителя аутентифицирует источник и целостность файла кода для СМ. Дополнительные параметры управления включены в файл кода для управления доступом к СМ.
- Хотя производитель должен всегда подписывать свои файлы кода, оператор кабельной сети может позже приложить свою подпись кода дополнительно к подписи производителя.

Модем CM должен проверить обе подписи в последовательности сертификатов, вплоть до корневого DOCSIS, прежде чем принять файл кода.

- Для выполнения этого процесса важны механизмы OSS инициализации и управления CM. Во время процессов инициализации и регистрации появляется возможность обновления кода CM. Загрузку кодов инициируют во время процессов инициализации и регистрации. Либо это можно выполнить обычной операцией, используя команду SNMP.

Файл кода создан с использованием структуры, совместимой с PKCS № 7, которая уже была описана в специальном формате для кабельных модемов DOCSIS. Структурой PKCS № 7, включенной в DOCSIS, является:

- изображение кода: обновление изображения кода;
- подпись проверки кода (CVS): цифровая подпись над изображением кода и любые другие атрибуты аутентификации, как это описано в структуре PKCS № 7 DOCSIS;
- сертификат проверки кода (CVC): структура сертификата, совместимая с X.509, которую используют для доставки и проверки правильности открытого ключа кода, который должен подтвердить подпись над изображением кода. Заслуживающая доверия администрация сертификата DOCSIS, чей открытый ключ уже хранится в кабельном модеме, подписывает этот сертификат. Сертификат X.509 определен в специальном формате для использования с кабельными модемами DOCSIS.

На рисунке B.1 показаны основные шаги, которые требуются для подписания изображения кода, когда файл кода подписан только производителем CM и когда файл кода подписан производителем CM, а также оператором кабельной сети.

В системе DOCSIS каждый кабельный модем должен получить заслуживающий доверия открытый ключ от администрации корневого сертификата DOCSIS. Создатель кода должен создать файл кода, подписывая изображение кода сертификата X.509 DOCSIS с использованием структуры цифровой подписи PKCS № 7 DOCSIS. Затем файл кода отправляют оператору кабельной сети. Оператору кабельной сети, получившему открытый ключ корневого DOCSIS, следует проверить, что этот файл кода поступил от заслуживающего доверия производителя DOCSIS и что файл не был модифицирован. В этом месте оператор кабельной сети имеет выбор загрузить файл кода на сервер tftp, "как есть", или добавить свою подпись и подпись оператора кабельной сети CVC к файлу кода. Во время процесса обновления кода CM должен иметь доступ к файлу кода на сервере tftp и проверить изображение кода перед инсталляцией.

Хотя CA корневого оборудования DOCSIS в последовательности сертификатов кабельного модема в настоящее время служит в качестве корневого CA загрузки ПО защиты, в будущем могут использоваться различные корневые CA. Поэтому модем CM НЕ ДОЛЖЕН считать, что производитель CVC и второй ответственный, подписавший CVC, выпустили корневой сертификат CA DOCSIS для последовательности сертификатов кабельного модема.

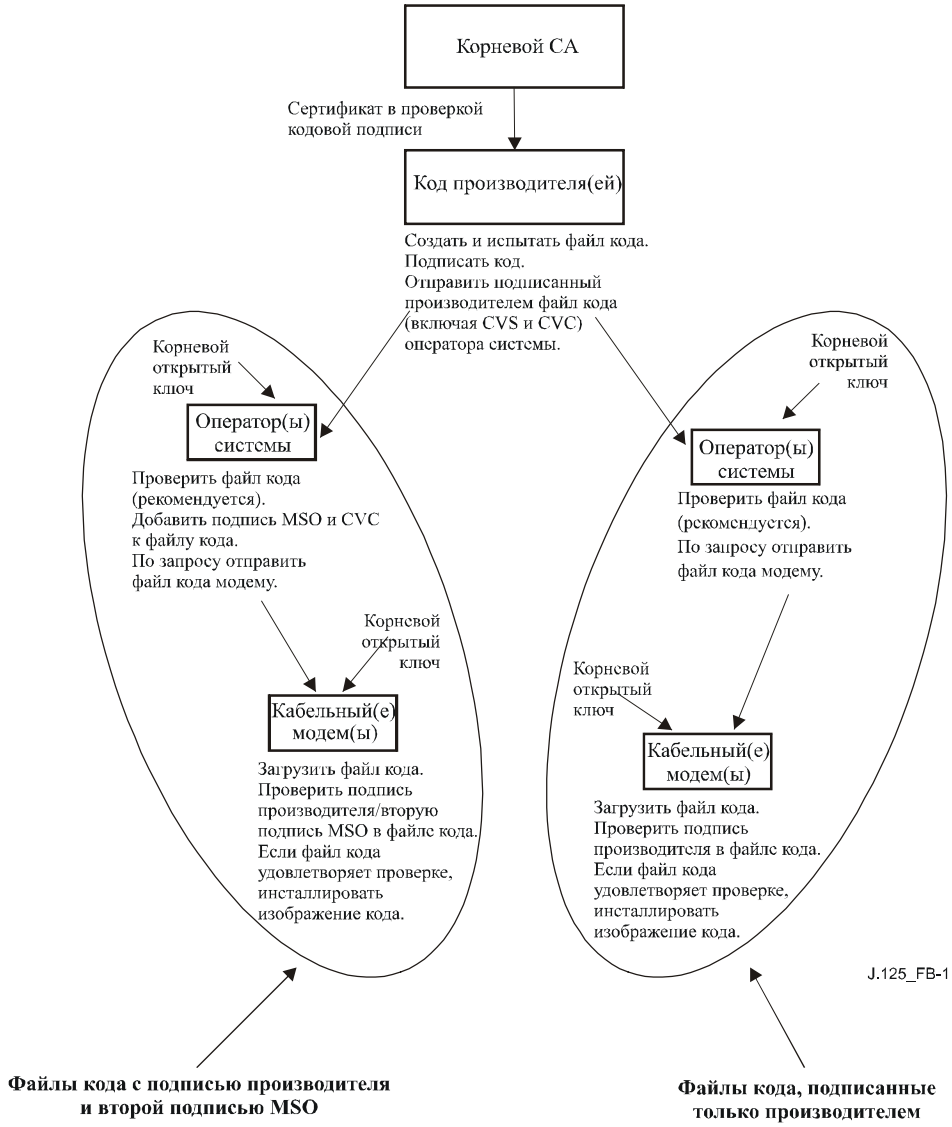


Рисунок B.1/J.125 – Иерархия проверки действительности типичного кода

B.3 Требования к обновлению кода

В следующих разделах описаны требования для поддержки обновления кода и процесс обновления. Все обновления кодов DOCSIS 1.1 или 2.0 должны быть подготовлены и проверены, как описано в этой Рекомендации. Все сертифицированные по DOCSIS 1.1 или 2.0 кабельные модемы должны проверить обновления кодов, согласно этой Рекомендации, независимо от того, работает ли модем по режимам совместимым DOCSIS 2.0, DOCSIS 1.1 или DOCSIS 1.0. Все сертифицированные по DOCSIS 1.1 и DOCSIS 2.0 кабельные модемы должны проверить обновление кода, согласно этой Рекомендации, независимо от того, включена или выключена базовая защита.

B.3.1 Требования к файлу кода

Для инкапсуляции кода в кабельный модем используют единственный файл. Этот файл кода является подписанным сообщением PKCS № 7 DOCSIS, которое включает:

1) подпись, удостоверяющую код производителя (CVS);

2) сертификат действительности кода производителя (CVC), подписанный корневой администрацией CA DOCSIS;

3) изображение кода (совместимое с назначением кабельного модема) в виде подписанного контента;

4) необязательную подпись в случае, когда операторы кабельной сети дополнительно подписывают файл кода:

   a) сертификат CVS операторов кабельной сети,

   b) сертификат оператора кабельной сети CVC, подписанный корневой администрацией CA DOCSIS;

5) необязательный открытый ключ корневой CA для проверки CVC;

6) необязательный(е) сертификат(ы) производителя.

Этот файл кода ДОЛЖЕН быть совместим с [PKCS № 7] и ДОЛЖЕН быть кодирован методом DER. Файл кода ДОЛЖЕН соответствовать структуре, показанной в таблице B.1. Пример показан в Дополнении I.

Таблица B.1/J.125 – Структура файла кода

Файл кода	Описание
PKCS № 7 Digital Signature{	
ContentInfo	
contentType	Подписанные данные
SignedData()	ЯСНО подписанное содержание; включает CVS и CVC X.509
}	
SignedContent{	
DownloadParameters {	Обязательный формат TLV (Тип 28), описанный в 7.2.2.28. (Длина нулевая, если отсутствуют sub-TLV.)
RootCAPublicKey()	Необязательный TLV для корневой CA открытый ключ для проверки CVC, отформатированный, согласно открытому ключу RSA, формат TLV (Тип 4), описанный в 7.2.2.4.
MfgCerts()	Дополнительный TLV для кодированных методом DER одного или более сертификата(ов) производителя. Каждый отформатирован, согласно формату сертификата CA TLV (Тип 17), описанного в 7.2.2.17.
}	
CodeImage()	Обновление изображения кода
}	

При загрузке Открытого ключа корневого CA и/или сертификата производителя как части файла кода CM, открытый ключ корневого CA и/или сертификаты CA производителя МОГУТ содержаться в поле RootCAPublicKey и/или в поле MfgCerts, как соответственно указано в таблице B.1, отдельно от действительного изображения кабельного модема, которое содержится в поле CodeImage.

Это дает возможность ясно отличать изображение кода от других параметров при загрузке файла кода. Это также позволяет изменять открытый ключ корневого CA, сертификаты CA производителя или параметры SignedData в файле загрузки кода без прерываний или изменения изображения кода, который получит кабельный модем. Это также позволяет проверить, что изображение кода не изменялось, даже если изменился файл загрузки кода из-за изменения открытого ключа корневого CA, сертификатов CA производителя или параметров SignedData.

B.3.1.1 Подписанные данные PKCS № 7 DOCSIS

Файл обновления ПО должен содержать информацию в подписанном типе контента данных PKCS № 7, как показано ниже. Эта структура, хотя и поддерживает используемую DOCSIS совместимость с [PKCS № 7], ограничена по формату для облегчения обработки, которую производит модем при проверке подписи. Подписанные данные PKCS № 7 ДОЛЖНЫ быть кодированы DER и точно соответствовать структуре, показанной в таблице B.2, за исключением любого изменения в порядке, который требуется для кодирования DER (*например*, расположения атрибутов SET OF). Модему CM следует отвергнуть подписи PKCS № 7, если подписанные данные PKCS № 7 не соответствуют кодированной DER структуре, представленной в таблице B.2.

Таблица B.2/J.125 – Подписанные данные PKCS № 7 DOCSIS

Поле PKCS № 7	Описание
Signed Data {	
version	Версия = 1
digestAlgorithmIdentifiers	SHA-1
contentInfo	
contentType	Данные (SignedContent объединенные с концом структуры [PKCS № 7])
certificates {	Сертификат действительности кода DOCSIS (CVC)
mfgCVC	ТРЕБУЮТСЯ все файлы кода
msoCVC	НЕОБЯЗАТЕЛЬНЫЙ; требует подписи оператора кабельной сети
} *end certificates*	
SignerInfo{	
MfgSignerInfo {	ТРЕБУЮТСЯ все файлы кода
version	Версия = 1
issuerAndSerialNumber	От подписавшего сертификат
issuerName	Отчетливое имя издателя сертификата
CountryName	US
organizationName	Спецификация интерфейса службы передачи данных по кабелю
organizationalUnitName	Кабельные модемы
commonName	Корневой сертификат администрации кабельного модема
certificateSerialNumber	Из CVC; целое число, размер (1..20) в октетах
digestAlgorithm	SHA-1
authenticatedAttributes	
contentType	Данные; contentType of signedContent
signingTime	UTCTime (GMT), YYMMDDhhmmssZ
messageDigest	Сжатое содержание, как описано в [PKCS № 7]
digestEncriptionAlgorithm	rsaEncription
encryptedDigest	
} *end mfg signer info*	
MsoSignerInfo {	НЕОБЯЗАТЕЛЬНЫЙ; требует подпись оператора кабельной сети
version	Версия =1
issuerAndSerialNumber	От издателя сертификата
issuerName	Отличительное имя издателя сертификата
CountryName	US
organizationName	спецификации интерфейса службы передачи данных по кабелю
organizationalUnitName	Кабельные модемы
commonName	Администрация корневого сертификата кабельного модема DOCSIS
certificateSerialNumber	Из CVC; целое число, размер (1..20) в октетах

Таблица B.2/J.125 – Подписанные данные PKCS № 7 DOCSIS

Поле PKCS № 7	Описание
digestAlgorithm	SHA-1
authenticatedAttributes	
contentType	Данные; contentType of signedContent
signingTime	UTCTime (GMT), YYMMDDhhmmssZ
messageDigest	Сжатое содержание, как описано в [PKCS № 7]
digestEncriptionAlgorithm	rsaEncription
encriptedDigest	
} end mso signer info	
} end signer info	
} end signed data	

B.3.1.1.1 Ключи подписания кода

Цифровая подпись PKCS № 7 использует алгоритм шифрования RSA [RSA3] с SHA-1 [FIPS-186-2]. Модуль ключа RSA для кода подписи состоит из 1024 битов, 1536 битов или 2048 битов длиной. Модем CM ДОЛЖЕН быть в состоянии проверить подписи файла кода DOCSIS, которые составлены с любым размером модулей. Открытой экспонентой является F4 (десятичное число 65537).

B.3.1.1.2 Формат сертификата проверки кода

Формат используют для CVC, что совместимо с X.509. Однако, в этом случае, структура X.509 ограничена для облегчения обработки, которую выполняет CM для проверки законности сертификата и для извлечения открытого ключа, который используют, чтобы проверить CVS. CVC должен кодироваться методом DER и точно соответствовать структуре, показанной в таблице B.3, за исключением любого изменения в порядке, который требуется для кодирования DER (*например*, расположения атрибутов SET OF). Модему CM следует отвергнуть CVC, если это не соответствуют кодированной DER структуре, представленной в таблице B.3.

CVC также требует дополнения идентификатора ID назначения ключа для "кодированного подписания" в поле применения ключа (KeyUsage).

```
-- extended Key usage extension OID and syntax
id-ce-exKeyUsage OBJECT Identifier ::= {id-ce 37}
ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId
KeyPuposeID ::= OBJECT Identifier
```

Код CVC DOCSIS ДОЛЖЕН содержать одно и только одно поле расширения: расширение применения расширенного ключа. Применение расширенного ключа ДОЛЖНО быть отмечено флагом как критическое. Применение расширенного ключа ДОЛЖНО содержать код назначения OID для кодированного подписания. Если расширение применения расширенного ключа отсутствует, или не отмечено флагом как критическое, или включает любой ключ назначения OID иной, чем или дополнительный к кодированному подписанию ID назначения, CM ДОЛЖЕН приостановить процесс проверки и сбросить CVC.

```
-- extended key purpose OIDs
id-kp-codeSigning OBJECT Identifier ::= { id-kp 3 }
```

Таблица B.3/J.125 – Проверка кода сертификата, совместимого с X.509 DOCSIS

Поле сертификата X.509	Описание
Certificate {	
tbsCertificate	
version	v3(2)
serialNumber	Целое число, размер (1..20) октетов
signature	SHA-1 с RSA, нулевые параметры
issuer	
countryName	US
organizationName	Спецификации интерфейса службы передачи данных по кабелю
organizationalUnitName	Кабельные модемы
commonName	Администрация корневого сертификата кабельного модема DOCSIS
validity	
notBefore	utcTime (GMT), YYMMDDhhmmssZ
notAfter	utcTime (GMT), YYMMDDhhmmssZ
subject	
countryName	<страна предмета собственности компании>
organizationName	<представитель компании, сделавший кодовую подпись>
organizationalUnitName	DOCSIS
commonName	Сертификат действительности кода
subjectPublicKeyInfo	
algorithm	Шифр RSA, нулевые параметры
subjectPublicKey	1024-битовый, 1536-битовый или 2048-битовый модули
extensions	
extKeyUsage	
critical	Истина
keypurposeId	id-kp-codeSigning
signatureAlgorithm	SHA-1 с RSA, нулевые параметры
signatureValue	
} *end certificate*	

B.3.1.1.3 Аннулирование сертификата

В этой Рекомендации не требуется и не определяется использования списков аннулированных сертификатов (CRL). Кабельному модему не требуется поддерживать CRL. Операторы кабельной сети могут пожелать определить и использовать CRL вне сети HFC DOCSIS, чтобы помочь управлению файлам кодов, которые поставляют им производители.

Однако существует метод аннулирования сертификатов, основанный на проверке стартовой даты сертификата (описанный в B.3.2.2). Этот метод требует, чтобы обновленный CVC был доставлен кабельному модему с обновленной проверкой времени старта. Как только CVC будет успешно проверен, проверка стартового времени по X.509 обновит текущее значение cvcAccessStart.

Для быстрой доставки обновленного значения CVC без требования от кабельного модема обработать обновленный код, CVC МОЖНО доставить либо конфигурацией файла CM, либо с помощью MIB SNMP. Формат CVC DOCSIS – тот же, что и у файла кода, файла конфигурации или MIB SNMP.

B.3.1.2 Подписанный контент

Поле подписанного контента файла кода содержит изображение кода и поле параметров загрузки, которое обычно содержит два дополнительные необязательные пункта: открытый ключ корневого CA DOCSIS и сертификат производителя.

Конечное изображение кода – это формат, совместимый с пунктом назначения кабельного модема. Для поддержки требований к подписи [PKCS № 7], содержание кода напечатано как данные; *т. е.* простой строкой октета. Формат окончательного изображения кода здесь не определен, а будет определен каждым производителем, согласно его требованиям.

Каждому производителю СЛЕДУЕТ построить свой код с дополнительными механизмами, которые проверят, является ли обновленное изображение кода совместимым с местом назначения кабельного модема. Модему CM НЕ СЛЕДУЕТ инсталлировать обновленное изображение кода то тех пор, пока не будет подтверждено, что изображение кода совместимо с CM.

При включении в поле подписанного контента, открытый ключ корневого CA DOCSIS предполагают заменить Открытым ключом корневого CA DOCSIS, который в настоящее время хранится в CM. Если загрузка кода и инсталляция, определенная в B.3.5.1, проходят успешно, то CM ДОЛЖЕН заменить текущий хранимый открытый ключ корневого CA DOCSIS на открытый ключ корневого CA DOCSIS, полученный в поле подписанного содержания. Это новый открытый ключ корневого CA DOCSIS будет затем использоваться для последующих проверок CVC.

При включении в поле подписанного контента сертификат(ы) производителя предполагают заменить тем(и) сертификатом(ами) производителя, которые в настоящее время хранятся в CM. Если загрузка кода и инсталляция, определенная в B.3.5.1, проходят успешно, то CM ДОЛЖЕН заменить текущий(е) хранимый(е) сертификат(ы) производителя на сертификат(ы) производителя, полученный(е) в поле подписанного содержания. Новый(е) сертификат(ы) производителя будет(ут) затем отправлен(ы) CMTS во время последующих инициализаций BPI+.

B.3.2 Контроль доступа файла

В дополнение к криптографическому контролю, который обеспечивает цифровая подпись и сертификат X.509, в файл кода включен специальный контроль значений для кабельного модема, чтобы проверить его прежде, чем будет проверено изображение кода. Условия, наложенные на значения этих параметров контроля, ДОЛЖНЫ выполняться раньше, чем CM будет проверять CVC или CVS, и должны принимать изображение кода.

B.3.2.1 Наименования организаций объектов

Кабельный модем должен распознавать одновременно до двух наименований, которые заслуживают доверия кодовой подписи представителя в поле объекта файла кода CVC. Эти наименования включают:

- Производителя кабельного модема: наименование производителя в поле объекта производителя CVC ДОЛЖНО точно соответствовать наименованию производителя, хранимому в не разрушаемой памяти CM производителя. Производитель CVC всегда должен быть включен в файл кода.
- Подписавшегося представителя: DOCSIS и производитель разрешают другой, заслуживающей доверия организации дополнительно подписать файлы кода, предназначенные их кабельным модемам. В большинстве случаев – это оператор кабельной сети, контролирующий текущую эксплуатационную область кабельного модема. Наименование организации подписывающего представителя связано с кабельным модемом через CVC этого представителя в файле конфигурации в процессе проверки кода кабельного модема при инициализации. Наименование организации подписывающего представителя в поле объекта CVC должно точно соответствовать полученному ранее наименованию организации подписавшего представителя при инициализации CVC и хранимого в памяти CM.

Модем CM МОЖЕТ сравнить наименования организаций, используя бинарное сравнение.

B.3.2.2 Варьируемый во времени контроль

Для поддержки процесса обновления кода CM ДОЛЖЕН держать два значения времени UTC, связанные с каждой кодовой подписью представителя. Один набор должен всегда храниться и поддерживаться производителем кабельного модема. Несмотря на то, что кабельному модему присвоен код подписавшего представителя, кабельный модем должен также хранить и поддерживать отдельный набор значений времени для этого представителя.

Эти значения использует для контроля файла кода доступа к кабельному модему индивидуального контроля законности кодов CVS и CVC. Этими значениями являются:

codeAccessStart: 12-байтовое значение времени UTC, отнесенное к среднему времени по Гринвичу (GMT).

cvcAccessStart: 12-байтовое значение времени, отнесенное к GMT.

Значение UTCTime в CVC должно быть выражено как среднее время по Гринвичу (GMT) и должно включать секунды. То есть оно должно быть выражено в следующей форме: YYMMDDhhmmssZ. Поле года (YY) должно интерпретироваться следующим образом:

- Если YY больше чем или равно 50, год интерпретируют как 19YY;
- Если YY меньше 50, год интерпретируют как 20YY.

Эти значения всегда должны соотноситься со средним временем по Гринвичу (GMT) с тем, чтобы заключительный знак ASCII (Z) мог быть удален при хранении модемом CM в виде codeAccessStart и cvcAccessStart. Модем CM должен поддерживать каждое из этих значений времени в формате, который содержит эквивалентную временную информацию и точность 12-значного формата UTC (т. е. YYMMDDhhmmss). Модем CM должен точно сравнивать эти хранимые значения со значениями времени UTC, доставляемыми модему в CVC. Эти требования обсуждаются далее в этой Рекомендации.

Значения codeAccessStart и cvcAccessStart, соответствующие производителю кабельного модема, НЕ ДОЛЖНЫ убывать. Значения codeAccessStart и cvcAccessStart, соответствующие подписавшему представителю НЕ ДОЛЖНЫ убывать то тех пор, пока не сменится представитель, а CM не удержит это изменившееся во времени значение контроля.

B.3.3 Инициализация обновления кода кабельного модема

Прежде чем кабельный модем сможет обновить код, модем следует инициализировать. Первым инициализирует кабельный модем его производитель. Каждый раз, когда кабельный модем регистрируются в сети DOCSIS, следует проверить текущее состояние его инициализации по сравнению с эксплуатационными нуждами. Может возникнуть необходимость повторной инициализации кабельного модема при регистрации; особенно если модем перемещали из одной сети в другую.

B.3.3.1 Инициализация производителя

На производителя возложена ответственность правильно инсталлировать в CM первоначальную версию кода.

Для поддержки проверки обновления кода, значения этих параметров должны быть загружены в не разрушаемую память CM:

1) organizationName производителя CM.
2) значения контроля производителя при изменениях во времени:
   a) значение инициализации codeAccessStart;
   b) значение инициализации cvcAccessStart.

Наименование организации производителя кабельного модема ДОЛЖНО быть всегда представлено в кабельном модеме. Значение organizationName производителя кабельного модема МОЖЕТ храниться в изображении кода кабельного модема. При нормальных условиях значение organizationName производителя НЕ СЛЕДУЕТ изменять, но эта Рекомендация не запрещает производителю изменять organizationName в памяти CM. Наименование производителя, которое используют для обновления кода, не обязательно используют в сертификате производителя DOCSIS.

Значения контроля во времени, codeAccessStart и cvcAccessStart должны быть инициализированы в сравнении со временем UTCTime, совместимым с проверкой времени запуска самого последнего кода CVC производителя. Эти изменяющиеся во времени значения должны периодически обновляться с помощью кодов CVC производителей, которые получает и проверяет кабельный модем.

Первоначально кабельный модем не должен распознавать подпись представителя.

B.3.3.2 Инициализация сети

Метод запуска и получения модемом CM файлов загрузки кода описан в [J.112-B] или [J.122]. Для поддержки проверки кода используют конфигурацию файла как средство аутентификации в процессе проверки кода. В файле конфигурации кабельного модема кабельный модем получает установки конфигурации, зависящие от проверки обновлений кода. Эти установки НЕ ДОЛЖНЫ использоваться до тех пор, пока CMTS не зарегистрирует успешно CM.

Конфигурации файла следует всегда включать с наиболее обновленным кодом CVC для места назначения кабельного модема, но если файл конфигурации используют для обновления кода, то следует включить код проверки сертификата (CVC), чтобы инициализировать кабельный модем для приема файлов кода, согласно этой Рекомендации. Независимо от того, требуется ли обновление кода, код CVC в файле конфигурации должен быть обработан кабельным модемом.

Файл конфигурации МОЖЕТ содержать:

- ни одного кода CVC;
- только код CVC производителя;
- только код CVC второго подписавшего (оператора кабельной сети);
- коды CVC обоих – производителя и второго подписавшего.

Прежде чем CM получит возможность обновить файлы кода в сети, он должен получить действующий код CVC в файле конфигурации и успешно зарегистрироваться в CMTS. Кроме того, если файл конфигурации кабельного модема не содержит действующий CVC, и отсутствует возможность обновления файлов кода, CM должен отвергнуть любую информацию в CVC, которая будет в последствии доставляться через SNMP.

Когда файл конфигурации кабельного модема содержит только действующий код CVC производителя, кабельный модем должен только запросить подпись производителя на файлах кода. В этом случае, CM НЕ ДОЛЖЕН принимать файлы кода, который имеют вторую подпись.

Когда файл конфигурации кабельного модема содержит код CVC второго подписавшего, модем использует код, чтобы инициализировать кабельный модем с подписью представителя. Если она действительна, то значение organizationName объекта CVC должно стать кодом подписавшего представителя, присвоенным кабельному модему. Чтобы в дальнейшем CM принял изображение кода, второй ответственный, в дополнение к подписи производителя кабельного модема, должен подписать файл кода.

Наименование организации производителя кабельного модема и изменяемых во времени значений контроля производителя должны быть всегда представлены в кабельном модеме. Если кабельный модем инициализирован, чтобы принять код второго ответственного с помощью дополнительной кодовой подписи представителя, наименование организация и соответствующие значения контроля во времени ДОЛЖНЫ храниться и поддерживаться во время эксплуатации. В памяти кабельного модема должно быть предусмотрено пространство для следующих значений контроля второго ответственного за подпись:

1) подписавшегося представителя organizationName;
2) значений контроля во времени:
   a) cvcAccessStart;
   b) codeAccessStart.

Установка этих значений производителя должна храниться в не разрушаемой памяти CM и не должна нарушаться во время отключения источника питания или во время перезагрузки CM. Когда модему присвоена вторая подпись, установки значений второго ответственного ДОЛЖНЫ сохраняться в

памяти CM. Модем CM МОЖЕТ удерживать в не разрушаемой памяти эти значения, которые не должны быть потеряны во время отключения источника питания или во время перезагрузки CM. Однако, при присвоении CM вторым представителем, код CVC всегда находится в файле конфигурации. Поэтому CM должен всегда получать значения контроля второго представителя во время фазы инициализации, и не требуется сохранять изменяемые во времени значения контроля при потере питания или при перезагрузке.

B.3.3.2.1 Обработка файла конфигурации CVC

Если код CVC включен в файл конфигурации DOCSIS 1.1 или 2.0, CM должен проверить CVC, прежде чем принять установки обновления кода, которые он содержит. При приеме CVC в файле конфигурации, CM должен выполнить следующие проверки и процедурные шаги. Если любая из следующих проверок потерпит неудачу, CM должен немедленно приостановить процесс проверки CVC и по возможности записать ошибку. Если файл конфигурации CM не включает CVC, который полностью проверен, CM НЕ ДОЛЖЕН загружать обновленные файлы кода ни с помощью файла конфигурации CM, ни с помощью MIB SNMP. Кроме того, если файлы конфигурации CM не включают код CVC, который соответственно проверен, модему CM не требуется обработка последующих кодов CVC, поступающих от MIB SNMP, и модем НЕ ДОЛЖЕН принимать информацию от последующих кодов CVC, поступающих от MIB SNMP.

При приеме CVC в файле конфигурации и после успешной регистрации на CMTS модем CM ДОЛЖЕН:

1) Проверить, что расширение применения расширенного ключа содержится в CVC, как это описано в B.3.1.1.2.

2) Проверить наименование организации объекта CVC.

   Если CVC – это CVC производителя (Тип 32), то:

   a) ЕСЛИ значение organizationName идентично наименованию производителя кабельного модема, то это – CVC производителя. В этом случае, CM должен проверить, что правильность стартового времени CVC производителя больше чем или равно текущему значению cvcAccessStart в CM.

   b) ЕСЛИ organizationName не идентично наименованию производителя кабельного модема, то этот CVC должен быть отвергнут, а ошибка занесена в журнал.

   Если CVC – это код CVC второго подписавшего код (Тип 33), то:

   a) ЕСЛИ значение organizationName идентично текущему подписанному представителем коду кабельного модема, то это – текущий. подписанный представителем код, и CM должен проверить, что стартовое время CVC представителя больше чем или равно текущему значению cvcAccessStart в CM.

   b) ЕСЛИ значение organizationName не идентично текущему подписанному представителем коду кабельного модема, то после того, как CVC будет проверен (и закончится регистрация), это наименование организации объекта должно стать для модема новым кодом с подписью представителя. CM НЕ ДОЛЖЕН принимать файл кода до тех пор, пока он не будет подписан производителем, а также вторым представителем.

3) Проверить законность подписи сертификата, используя ключ корневого DOCSIS, который имеется в CM. Проверки подписи CVC должны установить источник и подтвердить доверие к параметрам CVC.

4) Обновить текущее значение cvcAccessStart CM, соответствующее объекту organizationName CVC (*т. е.* производитель или код подписавшего представителя), проверкой значения стартового времени, найденному из действующего CVC. Если при проверке значение стартового времени будет больше, чем текущее значение codeAccessStart CM, то обновить значение codeAccessStart CM проверкой значения стартового времени. Модему CM СЛЕДУЕТ отбросить любые остатки CVC.

B.3.3.2.2 Обработка CVC SNMP

Модем CM ДОЛЖЕН обрабатывать сеть SNMP, поставляющую коды CVC, при обновлении файлов кода. В противном случае все доставленные SNMP файлы CVC должны отвергаться. При проверке кода CVC, полученного из сети SNMP, CM ДОЛЖЕН выполнить следующие поверки и процедурные шаги. Если любая из следующих проверок потерпит неудачу, CM ДОЛЖЕН немедленно приостановить процесс проверки CVC и по возможности записать ошибку и удалить все остатки процесса на этом этапе.

Модем CM ДОЛЖЕН:

1) Проверить, что расширение применения расширенного ключа содержится в CVC, как это описано в B.3.1.1.2.
2) Проверить наименование организации объекта CVC.
   a) ЕСЛИ значение organizationName идентично наименованию производителя кабельного модема, то это – CVC производителя. В этом случае, CM должен проверить, что правильность стартового времени CVC производителя больше чем или равно текущему значению cvcAccessStart в CM.
   b) ЕСЛИ значение organizationName идентично текущему коду подписавшегося представителя, то это – текущий код CVC подписавшегося представителя, и стартовое время должно быть больше, чем текущее значение cvcAccessStar, которое поддерживает CM.
   c) ЕСЛИ organizationName не идентично наименованию производителя кабельного модема или текущему коду подписавшегося представителя, то CM должен немедленно отвергнуть этот код CVC.
3) Проверить законность подписи сертификата, используя ключ корневого DOCSIS, который имеется в CM. Проверки подписей CVC должны установить источник и подтвердить доверие к параметрам CVC проверкой стартового времени.
4) Обновить текущее значение cvcAccessStart объекта проверкой значения стартового времени, найденного из действующего CVC. Если при проверке значение стартового времени окажется больше текущего значения codeAccessStart, то обновить значение codeAccessStart CM проверкой стартового времени. Все параметры сертификата ЗА ИСКЛЮЧЕНИЕМ проверки времени старта, более не требуются и должны быть отброшены.

B.3.4 Требования к подписанию кода

Следующие процедуры ДОЛЖНЫ последовать при подписании файлов кода.

B.3.4.1 Требования администрации сертификата (CA) DOCSIS

В дополнение к сертификату производителя DOCSIS, выпущенному производителем, как описано ранее в этой Рекомендации, корневая CAeDOCSIS должна выпустить сертификаты с подписанным кодом, который называется "Код проверки сертификатов" (CVC).

Код проверки сертификата (CVC) поставляется администрацией CA DOCSIS и подписывается корневым ключом DOCSIS (DRK). CVC, подписанные CA DOCSIS, должны быть в точности такими, как это определено в B.3.1.1.2, и использоваться только для поддержки кодовых подписей кабельных модемов DOCSIS. Администрация CA DOCSIS НЕ ДОЛЖНА подписывать никакой CVC, пока он не будет идентичен формату, определенному в этом разделе. Перед подписанием CVC, администрация CA DOCSIS должна проверить, что кодовая подпись представителя аутентична и действительно является кодовой подписью представителя.

Администрация CA DOCSIS должна быть ответственна за регистрацию наименований авторизованных кодовых подписей представителей. Кодовые подписи представителей включают производителей CM и операторов кабельных сетей, которые будут также подписчиками изображений кодов кабельных модемов. Администрация CA DOCSIS обязана гарантировать, чтобы наименование организации каждого представителя в кодовой подписи отличались. Следующее руководство должно действовать при написании наименований организаций со-подписчиками кодов:

- Наименование организации, использованной, чтобы идентифицировать себя в качестве представителя со-подписчика кода в CVC, должно быть присвоено DOCSIS.

- Наименование должно быть печатным строго из восьми шестнадцатеричных знаков, которые единственным образом отличают кодовую подпись представителя от подписей других.
- Каждый шестнадцатеричный знак в наименовании должен быть выбран из набора знаков 0-9 (0x30-0x39) или A-F (0x41-0x46).
- Строка, состоящая из восьми нулевых знаков не допускается и НЕ ДОЛЖНА использоваться в CVC.

B.3.4.2 Требования производства

Чтобы подписать свои файлы кода, производитель ДОЛЖЕН получить действующий CVC от CA DOCSIS. Все изображения кодов производителя, предоставленные оператору кабельной сети для удаленного обновления CM на сети HFC DOCSIS, ДОЛЖНЫ быть подписаны, согласно требованиям, определенным в этой Рекомендации.

При подписании файл кода, производитель МОЖЕТ не обновлять значение signingTime [PKCS № 7] в информации, подписанной производителем. Данная Рекомендация требует, чтобы значение signingTime [PKCS № 7] было равно или больше чем законное время старта CVC. Если производитель использует значение signingTime, равное законному времени старта CVC при подписании серии файлов кода, то эти файлы кода могут использоваться и повторно использоваться. Это позволяет оператору кабельной сети использовать файл кода либо для обновления, либо для новой загрузки версий кодов производителей кабельных модемов. Эти файлы кода будут действующими до тех пор, пока новый код CVC не будет создан и получен кабельным модемом. Рекомендуется, чтобы производитель подписал свои файлы кода таким образом, который допускает DOCSIS и стратегия защиты производителя (см. B.4).

Чтобы предохранить пространство памяти, CM МОЖЕТ внутренне представить имя подписавшего представителя в альтернативном формате, настолько длинном, как и вся информация, которая поддерживается, а оригинальный формат может быть воспроизведен, например, как 32-битовое ненулевое целое число со значением 0, представляющим отсутствие кодовой подписи представителя.

B.3.4.3 Требования оператора кабельной сети

Оператор кабельной сети DOCSIS должен получать ПО обновленных файлов кода от производителя. Используя корневой открытый ключ DOCSIS, оператору кабельной сети следует подтвердить. что изображение кода встроено заслуживающим доверия производителем. Оператор кабельной сети может перепроверить файл кода, в любое время, повторяя этот процесс.

Оператор кабельной сети имеет опцию второй подписи изображения кода, предназначенного для кабельного модема на своей сети. Чтобы сделать это, оператор кабельной сети подписывает содержание файла, согласно стандарту подписи [PKCS № 7], и включает CVC, подписанный DOCSIS. Для оборудования DOCSIS не требуется дополнительной подписи файлов кода оператором кабельной сети, но если оператор кабельной сети следует всем правилам, определенным в этой Рекомендации для подготовки файл кода, кабельный модем ДОЛЖЕН их принять.

Все изображения кодов, загруженные в CM из сети HFC DOCSIS, ДОЛЖНЫ быть подписаны, согласно требованиям этой Рекомендации.

B.3.5 Требования проверки кода

Обновленный код НЕ ДОЛЖЕН инсталлироваться до тех пор, пока не будет обнаружено, что код заслуживает доверия, согласно процессу проверки, описанному в этой Рекомендации.

Модем CM ДОЛЖЕН быть в состоянии обработать цифровую подпись [PKCS № 7] и сертификат DOCSIS X.509, как описано в этой Рекомендации. CM не должен поддерживать полный диапазон спецификаций [PKCS № 7] и X.509.

B.3.5.1 Этапы проверки кода кабельного модема

При загрузке кода CM должен выполнять проверки, представленные в этом разделе. Если любая из этих проверок окончится неудачей или если любой подраздел файла кода будет отвергнут из-за неправильного форматирования, CM должен немедленно приостановить процесс загрузки, записать ошибку, если это возможно, удалить все остатки этого этапа процесса и продолжать работу с

существующим кодом. Проверки могут выполняться в любом порядке до тех пор, пока не будут выполнены все представленные в этом разделе соответствующие проверки:

1) СМ ДОЛЖЕН подтвердить информацию подписи производителя, проверив что:
   a) значение signingTime [PKCS № 7] равно или больше, чем значение codeAccessStart производителя, которое в данный момент поддерживает СМ;
   b) значение signingTime [PKCS № 7] равно или больше, чем проверенное временем старта значение CVC производителя;
   c) значение signingTime [PKCS № 7] меньше чем или равно проверенному временем окончания значению CVC производителя.
2) Модем ДОЛЖЕН подтвердить CVC производителя, проверив что:
   a) объект organizationName CVC идентичен наименованию производителя, которое в данный момент находится в памяти СМ;
   b) правильность времени старта CVC равна или больше, чем значение cvcAccessStart производителя, которое в данный момент используется в СМ;
   c) расширение применения расширенного ключа в CVC такое, как описано в B.3.1.1.2.
3) СМ ДОЛЖЕН подтвердить подписи сертификата, используя корневой ключ DOCSIS, поддерживаемый СМ. Проверки подписей должны устанавливать подлинность источника открытого кода проверки ключа (CVK) и подтвердить доверие к ключу. Как только доверие будет установлено по CVK производителя, проверять оставшиеся параметры сертификата, ЗА ИСКЛЮЧЕНИЕМ проверки времени старта, более не требуются и их следует отбросить.
4) СМ ДОЛЖЕН проверить подписи файл кода производителя.
   a) СМ должен выполнить новое хэш-кодирование SHA-1 над SignedContent. Если значение messageDigest не соответствует новому хэш, СМ должен рассматривать подписи на файле кода как недействительные.
   b) Если подписи не подтверждены, то все компоненты файла кода (включая изображение кода) и любые значения, полученные в процессе проверки должны быть отвергнуты, и их следует немедленно удалить.
5) При проверке подписи производителя и подписи представителя требуется:
   a) СМ ДОЛЖЕН подтвердить информацию второй подписи, проверив что:
      1) информация о второй подписи включена в файл кода;
      2) значение signingTime [PKCS № 7] равно или больше чем соответствующее значение codeAccessStart, которое в данный момент поддерживает СМ;
      3) значение signingTime [PKCS № 7] равно или больше чем проверенное временем старта соответствующее значение CVC производителя;
      4) значение signingTime [PKCS № 7] меньше чем или равно проверенному временем окончания соответствующему значению CVC производителя.
   b) СМ ДОЛЖЕН подтвердить код CVC второй подписи, проверив что:
      1) объект organizationName CVC идентичен наименованию организации, которое в данный момент находится в памяти СМ;
      2) правильность времени старта CVC равна или больше, чем значение cvcAccessStart, которое в данный момент используется в СМ для соответствующего объекта organizationName;
      3) расширение применения расширенного ключа в CVC такое, как описано в B.3.1.1.2.
   c) СМ ДОЛЖЕН подтвердить подписи сертификата, используя корневой ключ DOCSIS, поддерживаемый СМ. Проверки подписей должны устанавливать подлинность источника открытого кода проверки ключа (CVK) и подтвердить доверие к ключу. Как

только доверие будет установлено по CVK, проверять оставшиеся параметры сертификата, ЗА ИСКЛЮЧЕНИЕМ проверки времени старта, более не требуются и их следует отбросить.

d) СМ ДОЛЖЕН проверить подписи файла кода второго представителя.

e) СМ ДОЛЖЕН выполнить новое хэш-кодирование SHA-1 над SignedContent. Если значение messageDigest не соответствует новому хэш, СМ должен рассматривать подписи на файле кода как недействительные.

f) Если подписи не подтверждены, то все компоненты файла кода (включая изображение кода) и любые значения, полученные в процессе проверки должны быть отвергнуты, и их следует немедленно удалить.

6) Если подписи производителя и дополнительно представителя проверены, изображение кода можно считать заслуживающим доверия, и инсталляцию можно производить. Перед инсталляцией изображения кода все прочие компоненты файла кода и любые значения, полученные в процессе проверки, за исключением значений signingTime [PKCS № 7] и проверки значений старта CVC, следует немедленно отбросить.

7) СМ может обновить свое ПО инсталлированием файла кода, согласно [J.112-B].

8) Если инсталляция кода закончилась неудачей, СМ ДОЛЖЕН отвергнуть значения signingTime [PKCS № 7] и значения старта CVC, которые только что были получены в файле кода. Необходимо следовать этапам, описанным в [J.112-B], для урегулирования условий неудачи.

9) Если инсталляция кода закончилась удачей, СМ ДОЛЖЕН обновить проверки производителя во времени с помощью значений, взятых из информации подписи и CVC производителя:

a) обновить текущее значение codeAcessStart значением signingTime [PKCS № 7];

b) обновить текущее значение cvcAccessStart значением правильности старта CVC.

10) Если инсталляция кода закончилась удачей и ЕСЛИ файл кода имел вторую подпись, СМ ДОЛЖЕН обновить проверки во времени второй подписи представителя значениями, взятыми из информации представителя второй подписи и CVC:

a) обновить текущее значение codeAccessStart значением signingTime [PKCS № 7];

b) обновить текущее значение cvcAccessStart значением правильности старта CVC.

B.3.6 Функциональная совместимость DOCSIS 1.0

Кабельные модемы DOCSIS 1.1 или 2.0 ДОЛЖНЫ проверить обновления кодов, согласно этой Рекомендации, даже при работе в среде DOCSIS 1.0.

Конфигурации файлов DOCSIS 1.0, предназначенные для кабельных модемов DOCSIS 1.1 или 2.0, ДОЛЖНЫ поддерживать в файле конфигурации требования, которые определены в этой Рекомендации.

Кабельные модемы DOCSIS 1.1 или 2.0 ДОЛЖНЫ получить совместимые файлы кода DOCSIS 1.1 или 2.0. Обновленные файлы проходят через систему DOCSIS 1.0 без изменений и не потребуют модификации обработки файл кода DOCSIS 1.0.

В среде DOCSIS 1.0, в которой кабельные модемы DOCSIS 1.1 или 2.0 получают файлы обновления кода, менеджеру SNMP СЛЕДУЕТ поддерживать базы MIB, определенные для проверки кода DOCSIS 1.1 или 2.0. Возможность использования базы MIB важна для нормальной работы и защиты процесса обновления кода DOCSIS 1.1 или 2.0.

B.3.7 Ошибки кодов

Ошибки кодов определены, чтобы отразить неудачи состояний, возможных во время процесса проверки кода. Описание и применение руководства для этих ошибок кодов можно найти в Дополнении H [SCTE23-3] или в Приложении D [SCTE79-2].

1) Ошибочный файл кода контролирует:
   a) объект organizationName CVC производителя не согласуется с наименованием производителя CM;
   b) объект organizationName CVC подписавшего код представителя не согласуется с текущим подписавшим код представителем CM;
   c) значение signingTime PKCS № 7 производителя меньше, чем текущее значение codeAccessStart в CM;
   d) значение проверенного времени старта PKCS № 7 производителя меньше, чем текущее значение cvcAccessStart в CM;
   e) проверенное время старта CVC производителя меньше, чем текущее значение cvcAccessStart в CM;
   f) значение signingTime PKCS № 7 производителя меньше, чем проверенное время старта CVC;
   g) пропавшее или неверное расширение расширенного ключа в CVC производителя;
   h) значение signingTime PKCS № 7 второго подписавшего меньше, чем текущее значение codeAccessStart в CM;
   i) проверенное время старта PKCS № 7 второго подписавшего меньше, чем текущее значение cvcAccessStart в CM;
   j) проверенное время старта CVC меньше, чем текущее значение cvcAccessStart в CM;
   k) значение signingTime PKCS № 7 второго подписавшего меньше, чем проверенное время старта CVC;
   l) пропавшее или неверное расширение расширенного ключа в CVC второго подписавшего представителя.
2) неудача проверки файла кода производителя CVC.
3) неудача проверки файла кода производителя CVS.
4) неудача проверки файла кода второго подписавшего CVC.
5) неудача проверки файла кода второго подписавшего CVS.
6) неправильный формат файла конфигурации CVC:
   a) пропавший или неверный атрибут key-usage.
7) неудача проверки файла конфигурации CVC.
8) Неправильный формат CVC SNMP:
   a) объект organizationName CVC производителя не согласуется с наименованием производителя CM;
   b) объект organizationName CVC подписавшего код представителя не согласуется с текущим подписавшим код представителем CM;
   c) проверенное время старта CVC меньше или равно соответствующему текущему значению cvcAccessStart объекта в CM;
   d) пропавший или неверный атрибут key-usage.
9) неудача проверки CVC SNMP.

B.4 Анализ защиты (Информативное)

Защита, которую обеспечивают персональные ключи, является решающим фактором защиты. Пользователи, авторизованные на кодовую подпись, т. е. производители и операторы, которые издали сертификаты проверки кодовой подписи (CVC) с помощью корневой CA DOCSIS, должны защищать свои персональные ключи. Злоумышленник с доступом к персональному ключу пользователя с авторизованной кодовой подписью может по желанию создать файлы кода, которые потенциально приемлемы для большого числа CM.

Защита против такой атаки побуждает оператора аннулировать сертификат, связанный с персональным ключом кодовой подписи, которая стала известна злоумышленнику. Чтобы аннулировать сертификат, оператор должен доставить каждому пораженному CM обновленный файл CVC с проверкой времени старта, которая будет новой по сравнению с этим временем у аннулированного сертификата. Новый CVC можно доставить с помощью поддерживаемых механизмов: конфигурации файла, кода файла или MIB SNMP. Новый CVC неявным образом аннулирует все сертификаты, у которых проверка времени старта более поздняя, чем у нового CVC.

Чтобы снизить уязвимость от таких атак, важно, чтобы оператор регулярно обновлял CVC в каждом CM, с периодичностью, сравнимой с тем, как часто оператор будет обновлять список аннулированных сертификатов (CRL), если такой список доступен. Регулярное обновление помогает сохранить временной интервал, в течение которого скомпрометированный ключ с кодовой подписью может быть полезен злоумышленнику. Независимо от того, в каком месте цикла обновления CVC вы находитесь, файл CVC следует также обновить, если есть подозрение, что ключ кодовой подписи скомпрометирован. Чтобы обновить CVC, пользователю необходим выпущенный DOCSIS CVC с проверкой времени старта более новой, чем у CVC в CM. Подразумевается, что корневой CA DOCSIS должен регулярно выпускать новые файлы CVC для всех авторизованных производителей кодовых подписей и операторов, чтобы обеспечить возможность обновления CVC. Администрации DOCSIS желательно установить стратегию выпуска новых CVC по расписанию, а операторам желательно скоординировать стратегию обновления с этим расписанием.

Когда CM делает попытку зарегистрироваться в сети первый раз или после длительного перерыва, важно, чтобы модем получил заслуживающий доверия CVC как можно быстрее. Это даст CM возможность получить самый новый из доступных CVC и запретить доступ для CVC, которые должны были считаться аннулированными с момента последней инициализации CM. Первая возможность модему CM получить заслуживающий доверия CVC заключается в его файле конфигурации. Если в файл конфигурации не входит действующий CVC, модем не должен запрашивать или иметь возможность удаленного обновления файлы кода. Кроме того, CM не должен принимать последующие файлы CVC, доставляемые с помощью MIB SNMP.

Чтобы смягчить возможность получения CM первоначального файла кода с повторением атаки, файлы кода включают значение времени подписания в структуру [PKCS № 7], которая может использоваться для указания времени, когда было подписано изображение кода. Когда CM получает файл кода с временем подписания, более поздним, чем последнее полученное изображение кода, модем должен обновить внутреннюю память этим значением. Модем CM не должен принимать файлы кода с более ранним временем подписания, чем это записанное внутреннее значение. Чтобы обновить CM новым файлом кода без закрытия доступа к предыдущим файлам кода, подписывающий администратор может не обновлять время подписания. Вследствие того, что многие файлы кода имеют одинаковое время подписания, оператору предоставляется возможность свободно понизить изображение кода CM до уровня предыдущей версии (то есть, до тех пор, пока не обновиться CVC). Это дает оператору ряд преимуществ, но следует оценивать эти преимущества сравнением с возможностью повторных атак на файл кода.

Без надежного механизма возвращения к предшествующей хорошей версии кода, любая схема обновления кода, включая схему в этой Рекомендации, имеет тот недостаток, что единственное вынужденное успешное обновление поврежденного изображения кода модемом CM может сделать CM бесполезным. Более того, неправильное изображение кода может привести к неправильной работе модема CM и повредить сеть. Такой модем может не поддаваться восстановлению при удаленном обновлении кода, поскольку неправильное изображение кода может не поддержать схему обновления.

Приложение C

Взаимодействие BPI/BPI+

Базовая защита плюс – это расширение первоначальных требований к базовой защите. По сравнению с первоначальной спецификацией там, где это было необходимо, эта спецификация добавила улучшения для повышения защиты системы и характеристик адресации. По возможности, исходная архитектура и конструкция базовой защиты были сохранены.

Эволюция возможностей DOCSIS 1.1 или 2.0 и базовой защиты плюс не была направлена на немедленную отмену систем DOCSIS 1.0 и использование базовой защиты. Переход DOCSIS к совместимым системам DOCSIS 1.1 и 2.0 может быть постепенным. Сейчас и впоследствии, система базовой защиты DOCSIS 1.0 и системы базовой защиты плюс DOCSIS 1.1 или 2.0 могут сосуществовать в рамках системы DOCSIS.

C.1 Взаимодействие DOCSIS v1.0/v1.1/v2.0

Требования взаимодействия BPI/BPI+ являются подмножеством общих требований взаимодействия DOCSIS v1.0/v1.1/v2.0, описанных в Приложении G [J.112-B] или [J.122]. Требования взаимодействия, описанные [J.112-B] или [J.122] для инициализации и регистрации следуют далее.

C.2 Требования взаимодействия DOCSIS BPI/BPI+

Требования взаимодействия BPI/BPI+ суммированы в таблице C.1. Системе базовой защиты плюс СЛЕДУЕТ быть обратно совместимой с базовой защитой, согласно этой таблице. Существует четыре пункта возможностей, взятых из спецификации базовой защиты и поддерживаемых этими требованиями взаимодействия.

1) Система окончания кабельного модема:
   a) CMTS BPI: базовая защита с 56-битовым DES. Должна принимать оба модуля открытого ключа – 768- и 1024-битовые.
   b) CMTS BPI – 40-битовый: базовая защита с 40-битовым DES. Должна принимать оба модуля открытого ключа – 768- и 1024-битовые. DES может работать только в 40-битовом режиме.
2) Кабельный модем:
   a) CM BPI: базовая защита с 56-битовым DES и модулями открытого ключа либо 768-битовым, либо 1024-битовым.
   b) CM BPI – 40-битовый: базовая защита с 40-битовым DES и модулями открытого ключа либо 768-битовым, либо 1024-битовым. DES может работать только в 40-битовом режиме.

Как описано в этой Рекомендации, базовая защита плюс вводит два дополнительные типа.

1) CMTS BPI+: базовая защита с 56-битовым DES. Должна принимать оба модуля открытого ключа – 768- и 1024-битовые.
2) CM BPI+: базовая защита с 56-битовым DES и 1024-битовым модулем открытого ключа.

Система CMTS и модем CM договариваются в сообщениях REG-REQ и REG-RSP о режиме совместимости BPI/BPI+, используя "возможности модема поддерживать конфиденциальность" TLV (тип 5.6). Требования взаимодействия BPI/BPI+ следующие:

   a) Система CMTS должна принять от модема CM во время авторизации открытые ключи с модулями как 768, так и 1024 битов.
   b) Если CM с базовой защитой плюс (CM BPI+) обеспечен файлом конфигурации типа DOCSIS 1.0, модем CM устанавливает "возможности модема поддерживать конфиденциальность" TLV (тип 5.6) либо поддерживать BPI (0), либо поддерживать BPI+ (1), в зависимости от возможности в данной ситуации (см. [J.112-B] пункт B.G.2.1, или [J.122] пункт G.1.1).

c) Если CMTS с базовой защитой плюс (CMTS BPI+) получает в сообщении от CM REG-REQ "возможности модема поддерживать конфиденциальность" TLV, установленную на поддержание BPI (тип 5.6, значение 0) или не тип 5.6 TLV, система CMTS ДОЛЖНА вернуться в совместимый режим работы [SCTE22-2] для связи с CM.

d) Если CMTS с базовой защитой плюс работает в системе, которая поддерживает модемы с BPI и BPI+, сервер TFTP должен включать следующие два типа конфигураций файлов:

- Конфигурацию файлов со всеми параметрами BPI (тип от 17.1 до 17.7) для модемов CM, приспособленных к режиму работы в BPI; и
- Конфигурацию файлов со всеми или частью параметров BPI+ для модемов CM, приспособленных к режиму работы в BPI+.

e) Если CM с базовой защитой плюс (CM BPI+) получает в сообщении от CMTS REG-RSP "возможности модема поддерживать конфиденциальность" TLV установленную на поддержание BPI (тип 5.6, значение 0) или не тип 5.6 TLV, модем CM ДОЛЖЕН вернуться в совместимый режим работы [SCTE22-2] для связи с CMTS.

ПРИМЕЧАНИЕ. – Как указано в Приложении B, модем CM DOCSIS 1.1 или 2.0 всегда проверяет загружаемое эксплуатационное ПО, независимо от установки поддержки конфиденциальности (тип 5.6) в сообщении REG-RSP и установки конфиденциальность включена (тип 4.7 или 29) в файле конфигурации CM.

Таблица C.1/J.125 – Матрица взаимодействия BPI/BPI+

	CM BPI	**CM BPI – 40-битовый**	**CM BPI+**
CMTS BPI	Внутренняя конфигурация BPI. 768- или 1024-битовые модули RSA.	768- или 1024-битовые модули RSA. ПО CMTS, нули TEK, биты 40-битового стандарта.	CM возвращается в режим BPI с 1024-битовым модулем RSA.
CMTS BPI 40-битовый	768- или 1024-битовые модули RSA. ПО CMTS нули TEK биты 40-битового стандарта.	768- или 1024-битовые модули RSA. Все 40 битов совместимости управляются чипами MAC.	CM возвращается в режим BPI с1024-битовым модулем RSA. ПО CMTS, нули TEK, биты 40-битового стандарта.
CMTS BPI+	CMTS возвращается в режим BPI. 768- или 1024-битовые модули RSA.	768- или 1024-битовые модули RSA. ПО CMTS, нули TEK, биты 40-битового стандарта.	Полный режим BPI+ или BPI, в зависимости от конфигурации файла и установки CMTS. 1024-битовый модуль RSA.

C.3 Анализ режима экспорта 40-битового DES BPI

Спецификация базовой защиты плюс обратно совместима с режимом экспорта 40-битового DES базовой защиты. Нагрузка совместимости ложится на CMTS. Не всем поставщикам оборудования DOCSIS приходится когда-нибудь работать с системой, имеющей блоки BPI с 40-битовыми DES. Поэтому совместимость является заботой отдельных производителей CMTS. Системе CMTS следует поддерживать обратную совместимость с режимом базовой защиты 40-битового DES. Если это выполняется, то должно выполняться, согласно этой Рекомендации.

a) Когда CMTS отправляет или принимает шифрованные данные между этой системой и CM, которые используют 40-битовый DES, то CMTS должна обнулить соответствующие биты ключей TEK, прежде чем зашифровывать и расшифровывать соответствующие данные трафика. Соответствующие биты TEK должны обнуляться, согласно требованиям базовой защиты 40-битовогоTEK.

b) Когда зашифрованный трафик должны передавать между CMTS только с возможностями 40-битового DES, а CM – с возможностями 56-битового DES, то система CMTS должна обеспечить совместимость 40-битового ключа TEK в ответ на сообщение запроса ключа CM.

Метод, который CMTS использует, чтобы распознать, какие модемы CM в системе имеют возможности 56-битового DES или только 40-битового DES, оставлен на усмотрение отдельных операторов систем и поставщиков CMTS, для того, чтобы наилучшим образом приспособиться к конкретной ситуации. Один из методов получения такой информации мог бы исходить от поставщиков модемов CM, основываясь на серийных номерах CM, MAC адресах, датах выпуска и некоторых других механизмах отслеживания устройств. Собранная один раз такая информация могла бы быть встроена в базу данных CMTS, хранимую для каждого CM.

Альтернативный метод получения этой информации связан с базой MIB BPI DOCSIS, предназначенной для этой цели.

C.4 Работа системы

C.4.1 Система CMTS с возможностями BPI

Система CMTS с возможностями BPI должна всегда обеспечивать модемы CM, используя файлы конфигурации типа TFTP DOCSIS 1.0 и установки конфигурации BPI. Как BPI, так и BPI+ модемов CM должны получать установки BPI, и каждый CM должен только пытаться зарегистрироваться как CM DOCSIS 1.0 с возможностями BPI. Если CM сообщает о возможностях модема BPI+ в запросе на регистрацию, система CMTS должна ответить удалением этих возможностей и форсировать совместимость CM с BPI.

C.4.2 Система CMTS с возможностями BPI+

Система CMTS с возможностями BPI+ DOCSIS 1.1 или 2.0 BPI+ ДОЛЖНА быть в состоянии работать в совместимых режимах с BPI и с BPI+, а также настраиваться, согласно возможностям каждого клиента CM. Когда CMTS обладает возможностями BPI+ и одновременно поддерживает BPI и BPI+ модемов CM, оба файла конфигурации, DOCSIS 1.0 и DOCSIS 1.1 или 2.0, должны быть доступны для установки конфигураций BPI+ и BPI в соответствующие модемы CM. Модем CM с возможностями BPI должен получить файл конфигурации DOCSIS 1.0 с установками BPI. Только тогда произойдет регистрация модема с возможностями BPI.

Приложение D

Обновление от BPI к BPI+

D.1 Гибридный кабельный модем с BPI+

Некоторые конструкции CM DOCSIS 1.0 могут поддерживать возможности BPI+ при обновлении ПО. Чтобы содействовать таким "гибридным модемам CM DOCSIS 1.0", источник [J.112-B] или [J.122] обеспечивает "возможности кодирования модема", которые гибридный модем может вложить в сообщение запроса на регистрацию, чтобы оговорить с CMTS свои возможности DOCSIS 1.1 или 2.0.

Гибридный кабельный модем DOCSIS 1.0 МОЖЕТ установить "возможности модема поддерживать конфиденциальность" на 1 (поддержка BPI Plus), если CM полностью совместим с BPI+, за исключением следующих пунктов:

- поддержка 56-битового DES, если CM поддерживает только 40-битовый DES;
- поддержка 1024-битового ключа RSA, если CM поддерживает 768-битовый ключ RSA;
- долговременная, только считываемая память для сертификатов CM, выпущенных производителем;
- шифрование объединенных пакетов, если "возможности модема поддерживать шифрование объединений" установлены на 0 (выключено);

- шифрования фрагментированных пакетов, если "возможности модема поддерживать шифрование фрагментированных пакетов" установлены на 0 (выключено);
- шифрование PHS (подавление полезной нагрузки заголовка) пакетов, если "возможности модема поддерживать шифрование подавления полезной нагрузки заголовка" установлены на 0 (выключено).

Гибридный кабельный модем с BPI+ будет взаимодействовать как с CMTS BPI+, так и с CMTS BPI с 56-битовым и 40-битовым DES. Требование к взаимодействию BPI/BPI+ в дополнение к Приложению C заключается в следующем:

a) Если гибридный кабельный модем с BPI+ поддерживает только 40-битовый DES и работает в режиме BPI+, то он ДОЛЖЕН отправить сообщение запроса Auth с атрибутом Security-Capabilities для описания 40-битового DES, а система CMTS ДОЛЖНА работать с модемом CM в режиме 40-битового DES, определенного в 10.1.

D.2 Процедура обновления

Функциональные возможности BPI+ МОГУТ быть загружены в CM DOCSIS 1.0 с помощью следующих процедур.

1) Загрузить ПО изображения кода в CM с возможностями BPI+ и MIB BPI+ с использованием функции загрузки ПО, определенной спецификацией DOCSIS 1.0. Сертификат CA производителя, подписанный персональным ключом корневой системы DOCSIS, внедрен в изображение кода ПО.
2) Установить в CM сертификат CM, подписанный персональным ключом производителя и открытым ключом CA корневой системы DOCSIS, используя MIB BPI+, если CM еще не имеет этой информации. Подробности объектов MIB BPI+ для этой операции должны быть определены [DOCSIS8].

ПРИМЕЧАНИЕ. – Модем CM может не работать ни в режиме BPI+, ни при установке "возможности модема поддерживать конфиденциальность" на 1 (поддерживать BPI Plus) до тех пор, пока в CM не будут установлены сертификат CM и открытый ключ CA корневой системы DOCSIS.

Дополнение I

Примеры сообщений, сертификатов и PDU

В этом Дополнении представлены численные примеры, которые могут быть полезны для применения этой Рекомендации. В этих примерах показаны типичные смены ключей: информация об авторизации, запрос на авторизацию, ответ на авторизацию, запрос ключа и ответ на запрос ключа. На каждом этапе приведены подробности криптографических расчетов и включены примеры сертификатов. Эти примеры также включают несколько пакетов PacketPDU, зашифрованных с использованием материала распределения и ввода ключей, полученного в примере смены ключей.

Это Дополнение является исключительно информативным и не составляет никакой части данной Рекомендации.

I.1 Обозначения

В приведенных здесь примерах, пакеты представлены как поток октетов, каждый октет в шестнадцатеричной записи, иногда с комментарием в виде текста. Порядок передачи октетов – слева направо и сверху вниз. Например, рассмотрим следующее представление пакета:

`00 01 02 03`	Описание № 1
`04 05`	
`06 07 08`	Описание № 2

Пакет состоит из 9 октетов, представленных в шестнадцатеричной записи как "00", "01", ..., "08". Октет, представленный как "00", передают первым, а октет, представленный как "08", передают последним.

При обсуждении примеров целые значения представлены либо в шестнадцатеричной записи с использованием префикса "0x", либо в десятичной записи без префикса. Например, шестнадцатеричная запись 0x12345 и десятичная запись 74565 представляют одно и то же целое число. Все целые числа – не отрицательные. Таким образом, 0xff представляет целое с неотрицательным значением 255.

Протокол BPKM генерирует и распределяет 8-октетные ключи DES и 16-октетные утроенные ключи DES без коррекции наименее значащего бита каждого октета для четности. При применениях извлекают 56-битоввый ключ из 8-октетного ключа и 112-битовый ключ из 16-октетного ключа, игнорируя значение наименее значащего бита каждого октета. В приведенных ниже примерах, ключи представлены без контроля чётности.

I.2 Информация идентификации

Модем CM отправляет следующую информацию идентификации:

0c 01 02 94	Заголовок Auth Info
11 02 91	Заголовок сертификата CA
30 82 02 8d 30 82 01 f6 . . . 81 87 19 61 72 20 19 1e	Сертификат CA

Поле кода имеет значение 0x0c, которое идентифицирует это как сообщение информации идентификации. Длина поля имеет значение 0x294 (660), которое представляет число октетов, которые следуют за длиной поля.

Единственным атрибутом является сертификат CA. Подробности сертификата приведены ниже.

I.2.1 Подробности

Поля сертификата CA в сообщении информации об авторизации разделяются следующим образом:

30 82 02 8d	Заголовок сертификата
30 82 01 f6	Заголовок TbsCertificate
a0 03 02 01 02	Версия
02 08 01 02 03 04 05 06 07 08	Серийный номер
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	Подписи
30 81 88	Заголовок издателя
31 0b 30 09 06 03 55 04 06 13 02 55 53	Наименование страны
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	Наименование организации
31 0f 30 0d 06 03 55 04 0b 13 06 44 4f 43 53 49 53	Наименование отделения организации
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	Наименование отделения организации
31 36 30 34 06 03 55 04 03 13 2d 4e 6f 72 74 65 6c 20 43 61 62 6c 65 20 4d 6f 64 65 6d 20 52 6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79	Общее наименование
30 1e	Проверка заголовка
17 0d 39 39 30 31 32 30 31 36 30 35 30 30 5a	Не ранее
17 0d 34 39 31 32 33 31 32 33 35 39 35 35 5a	Не позднее
30 81 88	Предмет заголовка
31 0b 30 09 06 03 55 04 06 13 02 55 53	Наименование страны
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	Наименование организации
31 0f 30 0d 06 03 55 04 0b 13 06 44 4f 43 53 49 53	Наименование отделения организации

31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	Наименование отделения организации
31 36 30 34 06 03 55 04 03 13 2d 4e 6f 72 74 65 6c 20 43 61 62 6c 65 20 4d 6f 64 65 6d 20 52 6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79	Общее наименование
30 81 9f	Заголовок открытого ключа объекта
30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00	Тип алгоритма открытого ключа
03 81 8d 00 30 81 89	Заголовок открытого ключа
02 81 81 00 af d1 86 c8 17 45 02 bc e5 59 b4 15 ac 95 87 7b 89 f5 8b f8 3b 8a 8b ef 67 cf 9e 00 47 d5 f1 06 42 55 36 a1 d1 8c dc cb 81 bb 31 8d 35 f7 6d 11 a0 91 9b 31 3d b9 71 38 46 15 c8 81 c4 51 06 7b d7 8a 70 be c1 28 0d 78 80 3c 44 a6 5e 35 5f 6e 46 2f 80 41 28 78 63 6c 86 cc d0 b3 58 ca bc 07 d5 19 3e 8a a2 1c 7e ff 0d 16 2b 0f bd a5 5e 60 93 64 09 80 24 76 ed e4 a9 e3 81 26 0c de 8a 89	Модуль открытого ключа
02 03 01 00 01	Порядок открытого ключа
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	Алгоритм подписи
03 81 81 00 81 4d db 31 e2 31 d2 6c f5 21 29 93 4a ce cb 6c fb 8b fc 3d ef 4b e8 4a 8a db f7 d8 e3 70 1d 3c ff ba 71 70 c4 82 24 9f 12 b5 d4 3e 3a 4d 20 64 2f ab 8b 05 27 9a 34 24 33 24 d4 7e bc 41 07 34 7a a6 51 12 29 55 e7 9b 5b e5 6b 79 bb 31 04 2f d1 c6 d3 7f 32 a2 b5 cc 99 23 09 97 1a 21 44 fa 25 3b f4 4b d6 00 cf e9 1b a9 be 9b 88 f8 90 fd 59 77 80 41 7d cb ca bf 81 87 19 61 72 20 19 1e	Значение подписи

В этом примере некоторые поля являются теми же самыми, что и во всех сертификатах CA. Эти поля следующие:

- версия: v3;
- подпись: SHA-1 с RSA, нулевые параметры;
- наименование объекта первого отделения организации: "DOCSIS";
- тип алгоритма открытый ключа: шифрование RSA, нулевые параметры;
- порядок открытого ключа: 3 октета целого числа, значение 0x10001;
- алгоритм подписи: SHA-1 с RSA, нулевые параметры.

Это пример собственноручной подписи сертификата CA. Наименование издателя и наименования объектов идентичны. В этом примере соответствующими полями наименований являются:

- наименование страны: "US";
- наименование организации: "Nortel";
- наименование первого отделения организации: "DOCSIS";
- наименование второго отделения организации: "Building 1, Andover MA";
- общее наименование: "Корневая администрация сертификата кабельного модема Nortel".

Остальные поля являются примерами значений. Некоторые из них:

- серийный номер: целое из 8 октетов, значение 0x0102030405060708 (другие сертификаты CA могут использовать другую длину);
- не ранее: 1999-01-20 16:05:00 GMT;
- не позже: 2049-12-31 23:59:55 GMT;
- модули открытого ключа: целое из 1024 битов, значение 0x00afd1...8a89 (другие сертификаты CA могут использовать целые длиной от 1024 до 2048 битов включительно);

- значение подписи: строка битов длиной 1024 битов, представляющих целое значение 0x00814d...191e. Другие сертификаты CA могут использовать строку битов длиной от 1024 до 2048 битов включительно; это совпадает с модулем издателя. Подписи вычисляют порциями сертификата, начиная с заголовка tbsCertificate и заканчивая порядком открытого ключа включительно.

I.3 Запрос на авторизацию

CM отправляет следующий запрос на авторизацию:

04 72 03 40	Заголовок Auth Request
05 00 ad	Заголовок идентификации CM
01 00 0c 30 30 30 30 30 30 31 32 33 34 35 36	Серийный номер
02 00 03 00 00 ca	ID производителя
03 00 06 00 00 ca 01 04 01	MAC адрес
04 00 8c 30 81 89 02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31 02 03 01 00 01	Открытый ключ RSA
12 02 7a	Заголовок сертификата CM
30 82 02 76 30 82 01 df . . . 19 c9 f1 dc 30 b8 d3 d5	Сертификат CM
13 00 0b	Заголовок возможности защиты
15 00 04 01 00 02 00	Список криптографического комплекта
16 00 01 01	Версия BPI
0c 00 02 22 60	SAID

Поле кода имеет значение 0x04, которое идентифицирует это как пакет запроса на авторизацию. Идентификатор поля имеет значение 0x72; это просто пример значения. Длина поля имеет значение 0x0340 (832), которое является числом октетов, которые следуют за длиной поля.

Первый атрибут – это идентификация CM. Это составной атрибут, состоящий из следующих податрибутов: Серийный номер, ID производителя, MAC адрес и Открытый ключ RSA. Для этих податрибутов показаны примеры значений.

Открытый ключ RSA кодирован методом DER и аналогичен примеру из пункта 2.2 [RSA2]. Модуль составляет 1024-битовое целое, представленное с использованием 0x81 (129) октетов. В этом примере, значение модуля:

```
0x00e0e06c8d ... caeed631.
```

Отметим, что 0x00 – это наиболее значащий октет модуля, а 0x31 – наименее значащий. Порядок – это целое, состоящее из 3 октетов и имеющее значение 0x010001.

Следующий атрибут – это сертификат CM. Подробности этого сертификата приведены ниже.

ПРИМЕЧАНИЕ. – Некоторые поля сертификата CM должны соответствовать податрибутам идентификации CM; этими податрибутами являются MAC адрес и открытый ключ RSA.

Следующий атрибут – это атрибут возможности защиты. Это составной атрибут, состоящий из Списка криптографического комплекта и версий BPI. В этом примере, в список включены два криптографических комплекта: 56-битовый DES без идентификации и 40-битовый DES без идентификации. Версия BPI – это BPI+.

Заключительный атрибут – это первичный идентификатор SAID модема CM, значение которого равно первичному SID. В этом примере, первичный SAID имеет значение 0x2260.

I.3.1 Детали сертификата CM

Поля сертификата CM в сообщении информации об авторизации распределяются следующим образом:

30 82 02 76	Заголовок сертификата
30 82 01 df	Заголовок tbsCertificate
a0 03 02 01 02	Версия
02 08 01 01 01 01 01 01 01 01	Серийный номер
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	Подпись
30 81 88	Заголовок издателя
31 0b 30 09 06 03 55 04 06 13 02 55 53	Наименование страны
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	Наименование организации
31 0f 30 0d 06 03 55 04 0b 13 06 44 4f 43 53 49 53	Наименование отделения организации
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	Наименование отделения организации
31 36 30 34 06 03 55 04 03 13 2d 4e 6f 72 74 65 6c 20 43 61 62 6c 65 20 4d 6f 64 65 6d 20 52 6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79	Общее наименование
30 1e	Заголовок проверки
17 0d 39 39 30 33 32 33 31 36 35 38 33 34 5a	Не ранее
17 0d 34 39 31 32 33 31 32 33 35 39 35 30 5a	Не позднее
30 72	Заголовок объекта
31 0b 30 09 06 03 55 04 06 13 02 55 53	Наименование страны
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	Наименование организации
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	Наименование отделения организации
31 15 30 13 06 03 55 04 03 13 0c 30 30 30 30 30 30 31 32 33 34 35 36	Общее наименование (Серийный номер)
31 1a 30 18 06 03 55 04 03 13 11 30 30 3a 30 30 3a 43 41 3a 30 31 3a 30 34 3a 30 31	Общее наименование (MAC адрес)
30 81 9f	Заголовок информации открытого ключа объекта
30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00	Тип алгоритма открытого ключа
03 81 8d 00 30 81 89	Заголовок открытого ключа

02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31	Открытый ключ модуля
02 03 01 00 01	Открытый ключ порядка
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	Алгоритм подписи
03 81 81 00 19 b0 2b e5 2c 37 4a af 34 cb c9 59 62 68 88 05 8a 91 5b d4 c6 fa 2e 19 ab 98 42 33 68 9d fc e4 76 23 84 8d 4a be ff bf 34 cf e0 fb 93 96 01 8b 89 d9 86 42 5e cf 6d e6 68 2e 44 99 56 6a cc f1 2c b9 5b 30 21 08 22 f5 11 b1 38 ba 6e b5 62 f0 3a dc f1 2e c4 61 95 2f 16 c8 27 63 b6 e8 69 a6 1c e1 4f 1a 8c 65 cb 57 5e 13 ce db 7f 27 f9 c1 6e bf 2f 75 77 9e a9 87 19 c9 f1 dc 30 b8 d3 d5	Значение подписи

В этом примере некоторые поля – те же, что и во всех сертификатах CM. Эти поля следующие:

- версия: v3;
- подпись: SHA-1 с RSA, нулевые параметры;
- наименование объекта первого отделения организации: "DOCSIS";
- тип алгоритма открытого ключа: шифрование RSA, нулевые параметры;
- порядок открытого ключа: 3 октета целого числа, значение 0x10001;
- алгоритм подписи: SHA-1 с RSA, нулевые параметры.

Наименование издателя и наименования объектов идентичны. В этом примере соответствующими полями наименований являются:

- наименование страны: "US";
- наименование организации: "Nortel";
- наименование первого отделения организации: "DOCSIS";
- наименование второго отделения организации: "Building 1, Andover MA";
- общее наименование: "Корневая администрация сертификата кабельного модема Nortel".

Остальные поля являются примерами значений. Некоторые из них:

- серийный номер: целое из 8 октетов, значение 0x0102030405060708 (другие сертификаты CA могут использовать другую длину);
- не ранее: 1999-03-23 16:58:34 GMT;
- не позднее: 2049-12-31 23:59:50 GMT;
- наименование страны объекта: "US";
- наименование организации объекта: "Nortel";
- наименование организационного отделения объекта: "Building 1, Andover MA";
- первое общее наименование объекта (серийный номер): "000000123456". Другие сертификаты CM могут использовать другую длину строки. Это значение соответствует атрибуту серийный номер сообщения запроса на авторизацию;
- второе общее наименование объекта (MAC адрес): "00:00:CA:01:04:01". Все сертификаты CM используют строку такой длины. Это значение соответствует атрибуту сообщения запроса на авторизацию;
- открытый ключ модуля: целое длиной 1024 битов, значение 0x00e0e0...d631 (другие сертификаты CM могут использовать целое длиной 768 или 1024 битов);

- значение подписи: строка битов длиной 1024 битов, представляющих целое значение 0x0019b0...d3d5. Другие сертификаты CM могут использовать строку битов длиной от 1024 до 2048 битов включительно; эта длина соответствует длине модуля издателя (выпустившего сертификат). Подписи вычисляют порциями сертификата, начиная с заголовка tbsCertificate и заканчивая порядком открытого ключа включительно.

I.4 Ответ на авторизацию

Система CMTS отправляет следующий ответ на авторизацию:

05 72 00 9f	Заголовок Auth Reply
07 00 80 a2 cb ad c8 34 27 71 47 06 d5 10 0c 07 94 90 bf e6 44 1b 0c 90 0d b4 ed 9c 39 aa 05 a0 c1 ef 54 4b cc fb 3a 7a 22 81 c0 dc c6 6e 39 a4 91 1c ba bf b0 ed 47 10 f2 f4 13 f9 09 33 c6 ae a3 45 67 c8 38 0f c3 9a 12 be d5 27 27 39 77 fb 98 03 39 50 39 99 f5 b6 ad b5 85 f9 16 d0 ff c6 2a ff 9f 38 73 6f 35 44 21 ad 9e e1 a5 91 4d 34 06 1d bb c9 b6 8f 8a 17 9e be c6 c9 40 eb 81 f0 62 d8 18	Ключ Auth
09 00 04 00 09 3a 80	Срок жизни ключа
0a 00 01 07	Номер последовательности ключей
17 00 0e	Заголовок дескриптора SA
0c 00 02 22 60	SAID
18 00 01 00	Тип SA
14 00 02 01 00	Криптографический набор

Поле кода имеет значение 0x05, которое идентифицирует это как ответ на пакет авторизации. Поле идентификатора имеет значение 0x72, соответствующее значению поля идентификатора запроса на авторизацию. Длина поля имеет значение 0x009f (159), которое представляет число октетов, следующих за длиной поля.

Первый атрибут – это ключ авторизации. Атрибут содержит ключ авторизации, который зашифрован RSA с использованием открытого ключа в сообщении запроса на авторизацию. Зашифрованный RSA ключ авторизации – это целое, состоящее из 0x80 (128) октетов. В этом примере, значение зашифрованного RSA ключа авторизации:

0xa2cbadc8 ... f062d818.

Отметим, что 0xa2 – это наиболее значащий октет зашифрованного RSA ключа авторизации, а 0x18 – наименее значащий. Подробности расчета шифрования RSA приведены ниже.

Второй атрибут – это Срок жизни ключа. В этом примере, это значение – 0x00093a80 (604800) секунд, или 7 дней.

Третий атрибут – это Номер последовательности ключей. В этом примере, это значение составляет 0x07.

Остальные атрибуты – это дескрипторы SA. Каждый дескриптор SA является составным атрибутом, состоящим из следующих податрибутов: SAID, Тип SA и криптографический набор. В этот пример включен простой дескриптор SA, соответствующий идентификатору SAID в запросе на авторизацию. Тип SA является первичным, а криптографический набор представляет 56-битовый DES без идентификации.

Каждый CM и CMTS находят ключ шифрования ключей и два сообщения идентификации ключей из ключа авторизации, используя хэширование. Подробности вычисления хэширования приведены ниже. Здесь в качестве примера приведены значения этих ключей:

Ключ авторизации	4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Ключ шифрования ключей	76 b4 d4 2f 14 98 59 6a ab fe 72 94 15 7c 7d 62
Сообщение идентификации ключа в восходящем направлении	fe b9 f1 e2 46 a7 6d 7c a7 7b 5e b0 98 25 fd 0b 57 ca 90 c7
Сообщение идентификации ключа в нисходящем направлении	93 d3 9d 70 c3 b6 f5 92 c4 6b d3 92 76 46 f4 f1 90 3a 52 fd

I.4.1 Подробности шифрования RSA

Система CMTS генерирует произвольные ключи авторизации из 20 октетов. В этом примере значение ключа авторизации:

```
4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
```

Ключ авторизации шифруют, используя схему RSAES-OAEP из [RSA3]. В этом разделе даны детали этой схемы применительно к данному примеру. Схема позволяет использовать функцию генерации маски (MGF), которая основана на хэшировании. Подробности приведены в дальнейшем разделе.

Ключ авторизации заполняют в 107-октетный блок DB:

```
DB =
da 39 a3 ee 5e 6b 4b 0d 32 55 bf ef 95 60 18 90 af d8 07 09 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01 42 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc ob 75
```

Чтобы сформировать DB, ключ авторизации предваряют октетом со значением 1, а результат помещают в последние 21 октетов блока. Первые 20 октетов блока представляют результат выполнения операции хэш над строкой нулевой длины. Эти 20 октетов имеют такое же значение в каждом ответе на авторизацию и не являются специальными для данного примера. Остальные 66 октетов блока устанавливают на 0.

Система CMTS генерирует произвольную строку из 20 октетов, которая называется SEED. Строку SEED генерируют независимо для каждого ответа на авторизацию. В этом примере SEED имеет значение:

```
SEED =
ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d
```

Строка SEED является входом в функцию MGF для генерации DB_MASK, блока из 107 октетов:

```
DB_MASK =
de 10 c9 59 41 c9 ea 72 a4 35 68 79 d2 53 85 db 13 7b a6 3b 37 ac 86 06 7c b5 ec
97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f
5d d5 f1 4d 25 8e 9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 c 3f 6e
ac 99 3a ae 14 3e 9a 8e df 3c 36 79 58 b2 fa 13 72 58 4c ca 04 a1 af c7 c4 62
```

DB и DB_MASK составляют вместе исключающее ИЛИ для создания MASKED_DB из 107 октетов:

```
MASKED_DB =
04 29 6a b7 1f a2 a1 7f 96 60 d7 96 47 33 9d 2d bc a3 a1 32 37 ac 86 06 7c b5 ec
97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f
5d d5 f1 4d 25 8e 9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f 6e
ac 99 3a ae 14 3f d4 0b f8 c3 f2 6b 2a 3c 9b 97 ac 91 6c 7c e4 c5 5f 7b cf 17
```

MASKED_DB является входом в функцию MGF для генерации SEED_MASK, блока из 20 октетов:

```
SEED_MASK =
b4 b6 f1 bf a6 b3 a1 7e 95 82 d3 b8 93 71 b6 7f 45 31 9e 82
```

SEED и SEED_MASK составляют вместе исключающее ИЛИ для создания MASKED_SEED из 20 октетов:

```
MASKED_SEED =
19 2a 5e 32 5e 95 5f d1 20 5d 2e 2d 4d 0f 21 b3 ac 7a f3 ef
```

MASKED_SEED и MASKED_DB объединяют, а результат предваряют простым октетом со значением 0. Этот результат представляет 128-октетный блок и называется EM:

```
EM =
00 19 2a 5e 32 5e 95 5f d1 20 5d 2e 2d 4d 0f 21 b3 ac 7a f3 ef 04 29 6a b7 1f a2
a1 7f 96 60 d7 96 47 33 9d 2d bc a3 a1 32 37 ac 86 06 7c b5 ec 97 d2 d0 9e 01 30
2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f 5d d5 f1 4d 25 8e
9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f 6e ac 99 3a ae 14 3f
d4 0b f8 c3 f2 6b 2a 3c 9b 97 ac 91 6c 7c e4 c5 5f 7b cf 17
```

Чтобы выполнить шифрование RSA, блок EM интерпретируют как целое значение:

0x00192a5e32 ... 5f7bcf17.

Отметим, что 0x00 – это наиболее значащий октет, а 0x17 – наименее значащий.

Шифрование RSA выполняют как операцию $Y = M^E \bmod N$, где:

M – это целочисленное значение блока EM (0x00192a5e32 ... 5f7bcf17); E – это целочисленное значение порядка открытого ключа RSA (0x010001); N – это целочисленное значение модуля открытого ключа RSA (oxe0e06c8d ... caeed631); Y – это целочисленное значение зашифрованного RSA ключа авторизации (0xa2cbadc8 ... f062d818).

I.4.2 Подробности дешифрирования RSA

В таблице I.1 перечислены параметры персонального ключа, который соответствует открытому ключу RSA в примере сообщения запроса на авторизацию.

Таблица I.1/J.125 – Параметры персонального ключа

Параметр	Свойство	Значение
D (персональный порядок)	$M^{DE} \bmod N = M$	6b 1f 1d 36 ec 77 7b 15 a9 c6 30 27 71 ae 92 62 3a 9f 67 47 d8 00 9d ca a0 0b f9 a6 0d be 54 3d 5a 6e be 25 25 bc d9 67 da 7b 80 5f a1 c6 75 67 dd 84 ba 4b 16 26 ba e9 fd 61 ab cd 49 e0 18 47 37 9f 56 08 2d d9 16 81 ff 7d d0 7e 01 8f d4 84 d3 e8 eb 27 48 c3 6c dc a9 01 b7 e5 24 28 d1 6c 67 03 a7 63 fb fa 79 d8 08 6a e1 de 3d 12 7a 36 20 25 01 d1 08 11 0c cd 80 44 3c fd c5 c4 db d1
P (первичный фактор)	N = PQ	f1 6b dd 2f dd d8 df 80 30 e6 9c d3 4e 46 5e 9f 42 62 b1 66 86 57 1b ca 87 9c cf fd 1c b6 26 76 95 35 bf 0b fb 51 af 0f 46 1c 5e cb 82 a0 83 bf 46 c9 3b d6 4e 7a 5d bf 03 05 69 27 31 6d 65 bd
Q (первичный фактор)	N = PQ	ee 74 cb a3 d0 90 2d 8a e9 e7 10 dd b4 65 2e 91 22 09 52 72 ab bd 32 31 4e d7 d0 2b 4b 13 57 20 6b f9 a4 57 b1 47 59 67 86 a6 8c 2c c1 f3 8b ba 8a 6b b1 62 5d 43 5a 71 db d0 33 43 97 99 17 85

Таблица I.1/J.125 – Параметры персонального ключа

Параметр	Свойство	Значение
D_p (порядок CRT)	$D_p = D \bmod (P - 1)$	a6 35 dc d2 57 aa 38 35 c9 74 fc 03 7e a0 74 04 b1 6f c1 33 14 ca 64 17 cb c5 ea 6c 18 98 4f 62 d4 d7 6b f0 93 d6 68 ef db 15 2d 2e 6f 80 93 33 dd 48 2e 2a 1d 5d a1 ad 20 27 59 7d e2 49 af 01
D_q (порядок CRT)	$D_q = D \bmod (Q - 1)$	cf f1 9c 30 33 cd b7 59 7f 96 57 f7 ee bb 99 bb 48 a2 36 7a f7 57 1a f1 32 df 32 92 be 7a 94 2d 1a db ed bb e7 45 e0 2a 4e 9a e8 7c 93 7a 4e 2c 93 4f 4c b6 09 bc 95 9f da df 9a 04 e4 ab c5 7d
U_p (постоянная CRT)	$PU_p \bmod Q = 1$	08 17 0c 11 bc aa 2f 96 80 8b 31 95 6d 2e b8 3c ee 2e 05 88 ab 9e fc 53 24 c4 04 b8 7e 1d 01 db 2d f2 2c 06 b0 cd 04 6b 1c 14 d8 d0 4f c9 a0 ae 1b c9 80 88 be 42 0a 52 4a ef 62 3c 8b dd c5 37

Каждое значение в таблице I.1 представляет октеты целого числа с наиболее значащим октетом, показанным первым. Например, персональный порядок D имеет целочисленное значение:

0x6b1f1d36 ... c5c4dbd1.

Модем CM может дешифровать ключ авторизации с – или без – использования китайской теоремы остатка (CRT). Дешифрование с использованием CRT является наиболее сложным, но может быть выполнено быстрее.

При дешифровании без использования CRT, модем CM выполняет операцию $M = Y^D \bmod N$. D – это персональный порядок из таблицы, а Y и N – величины, описанные в предыдущем разделе. Результирующее значение соответствует значению M в предыдущем разделе, которое является целочисленным значением блока EM, сформированного системой CMTS. Модем CM декодирует ключ авторизации из EM с помощью инвертированной процедуры, использованной системой CMTS для формирования EM, как описано в [RSA3].

Чтобы дешифровать, используя CRT, модем CM сначала вычисляет две промежуточные величины:

$$A = Y^{Dp} \bmod P;$$

$$B = Y^{Dq} \bmod Q.$$

P и Q являются первичными коэффициентами модуля, а D_p и D_q – персональными порядками, связанными с этими коэффициентами, причем все значения взяты из таблицы. CM вычисляет значение M как:

$$M = A + ((B - A)U_p \bmod Q)P$$

U_p – это константа, полученная из первичных коэффициентов со значениями, взятыми из таблицы. Результирующее значение M соответствует значению, которое можно было бы вычислить, используя операцию $M = Y^D \bmod N$.

I.4.3 Подробности хэширования

Ключ авторизации хэшируют, используя алгоритм SHA-1 [FIPS-180-2], чтобы получить ключ шифрования ключей (KEK), сообщение идентификации ключа в восходящем направлении и сообщение идентификации ключа в нисходящем направлении.

Здесь представлено обсуждение вычисления хэш с использованием таблицы, в которой показан вход функции хэш и результирующее значение хэш. Для сравнения в таблице описан пример из Приложения B [FIPS-180-2]:

Вход хэш	61 62 63 64 62 63 64 65 63 64 65 66 64 65 66 67 65 66 67 68 66 67 68 69 67 68 69 6a 68 69 6a 6b 69 6a 6b 6c 6a 6b 6c 6d 6b 6c 6d 6e 6c 6d 6e 6f 6d 6e 6f 70 6e 6f 70 71
Значение хэш	84 98 3e 44 1c 3b d2 6e ba ae 4a a1 f9 51 29 e5 e5 46 70 f1

I.4.3.1 Ключ KEK

KEK вычисляют, используя следующий расчет хэш:

Вход хэш	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 5 3 53 53 53 53 53 53 53 53 53 53 53 53 53 53 4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Значение хэш	76 b4 d4 2f 14 98 59 6a ab fe 72 94 15 7c 7d 62 b0 df e6 3b

Входом является октет 0x53, который повторяется 64 раза, за ними следуют 20 ключей авторизации. Порядок, в котором сжимают октеты ключа авторизации, такой же, как и порядок, в котором они появляются в блоке шифрования EM.

Значение хэш занимает длину в 20 байтов. Первые 16 байтов – это KEK.

I.4.3.2 Сообщение ключей идентификации

В восходящем направлении сообщение ключа идентификации находят, используя следующее вычисление хэш:

Вход хэш	5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Значение хэш	fe b9 f1 e2 46 a7 6d 7c a7 7b 5e b0 98 25 fd 0b 57 ca 90 c7

Входом является октет 0x53, который повторяется 64 раза, за ними следуют 20 октетов ключа авторизации. Порядок, в котором сжимают октеты ключа авторизации, такой же, как и порядок, в котором они появляются при вычислении KEK.

Значение хэш занимает длину в 20 октетов. 20 октетов в восходящем направлении составляют сообщение ключа идентификации.

В нисходящем направлении сообщение ключа идентификации вычисляют, используя следующий расчет хэш:

Вход хэш	3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Значение хэш	93 d3 9d 70 c3 b6 f5 92 c4 6b d3 92 76 46 f4 f1 90 3a 52 fd

Это аналогично вычислению в восходящем направлении за исключением того, что значение 0x3a заменяют значением 0x5c.

I.4.3.3 Функция генерации маски

Функцию генерации маски (MGF) создают вне операции хэш SHA-1. Каждая хэш операция генерирует 20 октетов данных маски. Число выполняемых операций хэш зависит от размера требуемой маски.

Величину SEED_MASK формируют, применяя MGF к MASKED_DB. Поскольку SEED_MASK составляет длину в 20 октетов, потребуется только одна операция хэш:

Вход хэш	04 29 6a b7 1f a2 a1 7f 96 60 d7 96 47 33 9d 2d bc a3 a1 32 37 ac 86 06 7c b5 ec 97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f 5d d5 f1 4d 25 8e 9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f 6e ac 99 3a ae 14 3f d4 0b f8 c3 f2 6b 2a 3c 9b 97 ac 91 6c 7c e4 c5 5f 7b cf 17 00 00 00 00
Значение хэш	b4 b6 f1 bf a6 b3 a1 7e 95 82 d3 b8 93 71 b6 7f 45 31 9e 82

Вход данных в операцию хэш составляет 107 октетов MASKED_DB, за которыми следуют четыре октета со значением 0. Выходом операции является значение SEED_MASK.

Величину DB_MASK находят, применяя MGF к SEED. Поскольку DB_MASK составляет длину в 107 октетов, потребуется шесть операций хэш:

Вход хэш	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 00
Значение хэш	de 10 c9 59 41 c9 ea 72 a4 35 68 79 d2 53 85 bd 13 7b a6 3b

Вход хэш	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 01
Значение хэш	37 ac 86 06 7c b5 ec 97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9

Вход хэш	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 02
Значение хэш	a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f 5d d5 f1 4d 25 8e

Вход хэш	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 03
Значение хэш	9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f

Вход хэш	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 04
Значение хэш	6e ac 99 3a ae 14 3e 9a 8e df 3c 36 79 58 b2 fa 13 72 58 4c

Вход хэш	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 05
Значение хэш	ca 04 a1 af c7 c4 62 3a df 6f 33 ec e2 cd 2c 7f b7 7e 48 19

Вход данных в каждую операцию хэш составляет 20 октетов SEED, за которым следует значение из четырех октетов. Это значение из четырех октетов представляет счет целочисленных значений 0, 1, 2, 3, 4, 5 последовательных операций хэш. Входы шести операций хэш объединяют в результат из 120 октетов, а первые 107 октетов этого результата образуют DB_MASK.

I.5 Запрос ключа

Модем CM отправляет следующий запрос ключа:

07 73 00 d0	Заголовок запроса ключа
05 00 ad	Заголовок идентификации CM
01 00 0c 30 30 30 30 30 30 31 32 33 34 35 36	Серийный номер
02 00 03 25 53 41	ID производителя
03 00 06 00 00 ca 01 04 01	MAC адрес
04 00 8c 30 81 89 02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31 02 03 01 00 01	Открытый ключ RSA
0a 00 01 07	Номер последовательности ключей
0c 00 02 22 60	SAID
0b 00 14 86 b8 33 b7 48 9c 4b a1 51 67 44 d7 a6 e6 ca 21 33 f5 22 9e	Сжатое описание HMAC

Поле кода имеет значение 0x07, которое идентифицирует это как пакет запроса ключа. Идентификатор поля имеет значение 0x73; это просто пример значения, полученного увеличением значения идентификатора в запросе на авторизацию. Длина поля имеет значение 0x00d0 (208), которое состоит из числа октетов, следующих за длиной поля.

Первым атрибутом является идентификация CM. Этот составной атрибут идентичен такому же в запросе на авторизацию.

Второй атрибут – это номер последовательности ключей, который идентифицирует ключ авторизации. Это значение идентично такому же в ответе на авторизацию.

Третий атрибут – это идентификатор SAID, для которого запрашивают ключ. Это значение SAID содержалось в ответе на авторизацию.

Заключительный атрибут – это сжатое сообщение HMAC. Это сообщение состоит из 20 октетов. Его вычисляют, используя сообщение идентификации ключа в восходящем направлении. Сжатое сообщение содержится после всех октетов пакета запроса ключа, исключая 23 октета самого атрибута HMAC Digest. Подробности вычисления сжатого сообщения приведены ниже.

I.5.1 Подробности сжатого сообщения HMAC

Сжатое сообщение HMAC вычисляют, используя метод идентификации HMAC, определенный в [RFC2104] с SHA-1 в качестве функции хэш. Примеры вычисления HMAC с использованием SHA-1 представлены в [RFC2202].

Здесь обсуждается вычисление HMAC с использованием таблицы, в которой показаны ключ, вход в функцию HMAC и результирующее сжатое сообщение HMAC. Для сравнения здесь приведена таблица, в которой описан случай тестирования № 2 HMAC-SHA-1 из примеров в [RFC2202]:

Ключ	4a 65 66 65
Вход HMAC	77 68 61 74 20 64 6f 20 79 61 20 77 61 6e 74 20 66 6f 72 20 6e 6f 74 68 69 6e 67 3f
Сжатое сообщен. HMAC	ef fc df 6a e5 eb 2f a2 d2 74 16 d5 f1 84 df 9c 25 9a 7c 79

Сжатое сообщение HMAC пакета запроса ключа вычисляют, используя следующий алгоритм вычисления HMAC:

Ключ	fe b9 f1 e2 46 a7 6d 7c a7 7b 5e b0 98 25 fd 0b 57 ca 90 c7
Вход HMAC	07 73 00 d0 05 00 ad 01 00 0c 30 30 30 30 30 30 31 32 33 34 35 36 02 00 03 25 53 41 03 00 06 00 00 ca 01 04 01 04 00 8c 30 81 89 02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31 02 03 01 00 01 0a 00 01 07 0c 00 02 22 60
Сжатое сообщен. HMAC	86 b8 33 b7 48 9c 4b a1 51 67 44 d7 a6 e6 ca 21 33 f5 22 9e

Ключ – это ключ идентификации сообщения в восходящем направлении. Вход состоит из всех октетов пакета запроса ключа, исключая атрибут HMAC Digest. Содержанием атрибута HMAC Digest являются октеты сжатого сообщения.

I.6 Ответ на запрос ключа

Система CMTS отправляет следующий ответ на запрос ключа:

08 73 00 68	Заголовок ответа на запрос ключа
0a 00 01 07	Номер последовательности ключей (ключей авторизации)
0c 00 02 22 60	SAID
0d 00 21	Заголовок параметров TEK
08 00 08 b6 4d 54 8c 3f 6b 25 69	Ключ TEK
09 00 04 00 00 a8 c0	Срок жизни ключа
0a 00 01 02	Номер последовательности ключей (TEK)
0f 00 08 81 0e 52 8e 1c 5f da 1a	DES CBC-IV
0d 00 21	Заголовок параметров TEK
08 00 08 5e bd 03 aa 5e d5 e2 94	Ключ TEK
09 00 04 00 01 51 80	Срок жизни ключа
0a 00 01 03	Номер последовательности ключей (TEK)
0f 00 08 25 35 67 c3 09 21 8c 2c	DES CBC-IV
0b 00 14 a5 e3 33 25 ea 72 f8 50 1c 2a b6 65 45 6b cc de 8b 4f 22 02	Сжатое сообщение HMAC Digest

Поле кода имеет значение 0x08, которое идентифицирует это как пакет ответа на запрос ключа. Идентификатор имеет значение 0x73, соответствующее значению в запросе ключа. Длина поля имеет значение 0x68 (104), которое является числом октетов, следующих за длиной поля.

Атрибут номер последовательности ключей идентифицирует ключ авторизации. Он соответствует этому значению в запросе ключа.

Атрибут SAID идентифицирует SAID, с которым поставляют TEK. Он соответствует этому значению в запросе ключа.

Включены атрибуты двух параметров TEK: первый – для старой генерации параметров ключей, а второй – для новой. Атрибут каждого параметра TEK является составным атрибутом, состоящим из следующих податрибутов: ключа TEK, срока жизни ключа, номера последовательности ключей и DES CBC IV.

Ключ TEK состоит из 8 октетов. Он содержит TEK, зашифрованный с использованием тройного алгоритма DES-ECB с ключом KEK, который находят из ключа авторизации. Подробности вычисления по тройному алгоритму DES-ECB приведены ниже.

Податрибут срок жизни ключа относится к TEK. В этом примере значение для старого ключа TEK составляет 0x0000a8c0 (43200) секунд, или 12 часов, а значение для нового TEK составляет 0x00015180 (86400) секунд, или 24 часа.

Податрибут номер последовательности ключей идентифицирует TEK. В этом примере значение для старого ключа TEK составляет 0x02, а значение для нового TEK составляет 0x03.

Податрибут DES CBC-IV состоит из 8 октетов. Он определяет вектор инициализации для использования с TEK.

Заключительный атрибут – это сжатое сообщение HMAC. Он состоит из 20 октетов. Атрибут вычисляют способом, аналогичным тому, который использован в ответе на запрос ключа, за исключением того, что используют ключ идентификации сообщения в нисходящем направлении, вместо восходящего направления. Подробности вычисления HMAC приведены ниже.

После того, как CM обработает пакет ответа на запрос ключа, CM и CMTS каждый поделят две генерации TEK и IV. Вот значения этих параметров для данного примера:

Старый TEK	`e6 60 0f d8 85 2e f5 ab`
Старый IV	`81 0e 52 8e 1c 5f da 1a`
Новый TEK	`b1 d7 4f c9 64 68 f7 58`
Новый IV	`25 35 67 c3 09 21 8c 2c`

I.6.1 Подробности шифрования TEK

Система CMTS генерирует произвольные ключи TEK из 8 октетов. В этом примере значение TEK:

`e6 60 0f d8 85 2e f5 ab.`

Это – первый ключ TEK в сообщении ответа на запрос ключа.

TEK шифруют, используя тройной алгоритм шифрования triple-DES-ECB. Зашифрованный ключ является ключом KEK:

`76 b4 d4 2f 14 98 59 6a ab fe 72 94 15 7c 7d 62.`

Тройной алгоритм шифрования triple-DES-ECB приведен здесь в понятиях нескольких итераций шифрования или дешифрования DES-ECB, описанных в [FIPS-81].

Здесь рассматривается операция шифрования или дешифрования DES-ECB, в которой используют таблицу, указывающую ключ, вход и выход. Для сравнения приведены таблицы, которые описывают пример из таблице B1 [FIPS-81]:

Режим	шифрование ECB
Ключ	`01 23 45 67 89 ab cd ef`
Вход DES	`4e 6f 77 20 69 73 20 74`
Выход DES	`3f a4 0e 8a 98 4d 48 15`

Режим	дешифрование ECB
Ключ	`01 23 45 67 89 ab cd ef`
Вход DES	`3f a4 0e 8a 98 4d 48 15`
Выход DES	`4e 6f 77 20 69 73 20 74`

ПРИМЕЧАНИЕ. – В [FIPS-81] рекомендуют, чтобы наименее значащий бит каждого октета в ключе настраивали таким образом, чтобы этот октет имел проверку на нечётность. Это видно на вышеприведенном примере ключа. Протокол BPKM не требует проверки на нечётность. BPKM генерирует и распределяет 8-октетные ключи DES произвольной четности, а также требует, чтобы применения игнорировали значение наименее значащего бита каждого октета.

Ключ TEK, зашифрованный тройным алгоритмом шифрования triple-DES-ECB, использует следующие операции DES-ECB:

Режим	шифрование ECB
Ключ	76 b4 d4 2f 14 98 59 6a
Вход DES	e6 60 0f d8 85 2e f5 ab
Выход DES	c3 94 31 f5 8d f9 1d bf

Режим	дешифрование ECB
Ключ	ab fe 72 94 15 7c 7d 62
Вход DES	c3 94 31 f5 8d f9 1d bf
Выход DES	44 b0 94 4e ab 04 4c 23

Режим	шифрование ECB
Ключ	76 b4 d4 2f 14 98 59 6a
Вход DES	44 b0 94 4e ab 04 4c 23
Выход DES	b6 4d 54 8c 3f 6b 25 69

Первая и третья операции – это операции шифрования DES-ECB. Ключ для каждой операции составляет первые восемь октетов KEK. Вторая операция – это дешифрование DES-ECB. Ключ – это последние восемь октетов KEK. Вход в первую операцию – это ключ TEK, который предстоит зашифровать. Вход во вторую операцию – это выход первой, а вход в третью операцию – это выход второй. Выходом третьей операции будет зашифрованный ключ TEK. Это передают в податрибуте ключа TEK в сообщении ответа на запрос ключа.

I.6.2 Подробности HMAC

Сжатое сообщение HMAC пакета с ответом на запрос ключа вычисляют методом, аналогичным методу вычисления пакета с запросом ключа. Этот ключ – ключ идентификации сообщения в нисходящем направлении. Ниже приведены подробности вычисления HMAC:

Ключ	93 d3 9d 70 c3 b6 f5 92 c4 6b d3 92 76 46 f4 f1 90 3a 52 fd
Вход HMAC	08 73 00 68 0a 00 01 07 0c 00 02 22 60 0d 00 21 08 00 08 b6 4d 54 8c 3f 6b 25 69 09 00 04 00 00 a8 c0 0a 00 01 02 0f 00 08 81 0e 52 8e 1c 5f da 1a 0d 00 21 08 00 08 5e bd 03 aa 5e d5 e2 94 09 00 04 00 01 51 80 0a 00 01 03 0f 00 08 25 35 67 c3 09 21 8c 2c
Сжатое сообщение HMAC	a5 e3 33 25 ea 72 f8 50 1c 2a b6 65 45 6b cc de 8b 4f 22 02

I.7 Шифрование пакета PDU

Первые 12 октетов пакета PDU, содержащие адреса назначения и источника Ethernet/802.3 (DA/SA), не шифруют. Оставшиеся октеты пакета PDU шифруют, используя режим DES-CBC со специальной обработкой оставшихся завершающих блоков, которые менее 64 битов. Комбинация обработки DES-CBC и блоков остатка гарантирует, что шифрование не изменит длину пакета. Ключ шифрования – это TEK, соответствующий номеру последовательности ключей расширенного заголовка конфиденциальности пакета.

Спецификация описывает обработку блока остатка следующим образом:

"Задан конечный блок, имеющий n битов, где n меньше 64; предпоследний зашифрованный блок – это блок, зашифрованный методом DES второй раз с использованием режима ECB, а наименее значащие n битов результата образуют с последними n битами полезной нагрузки исключающие ИЛИ для генерации заключительного зашифрованного блока. В особом случае, когда полезная нагрузка данных пакетов PDU меньше 64 битов, вектор инициализации шифруют методом DES, а крайние левые n битов результирующего шифрованного текста, соответствующие числу битов полезной нагрузки, образуют с n битами полезной нагрузки исключающие ИЛИ для генерации короткого зашифрованного блока."

Альтернативное описание этой процедуры, которое эквивалентно описанию в спецификации, выглядит следующим образом:

Задан конечный блок, имеющий n битов, где n меньше 64; n битов дополняют до блока в 64 бита, присоединяя 64-n битов с произвольным значением вправо от n битов полезной нагрузки. Результирующий блок шифруют методом DES, используя режим CFB64, с предпоследним зашифрованным блоком, который служит вектором инициализации для операции CFB64. Крайние левые n битов результирующего шифрованного текста используют как короткий зашифрованный блок. В особом случае, когда полезная нагрузка данных пакетов PDU меньше 64 битов, процедура остается той же самой, что и для короткого заключительного блока с добавлением вектора инициализации, который служит вектором инициализации для операции DES-CFB64.

Альтернативное описание порождает такой же зашифрованный текст, что и описание в спецификации. В альтернативном описании, однако, нет упоминания о комбинации шифрования ECB с исключающими ИЛИ. Эти операции являются внутренними для CFB64, так же как они являются внутренними для CBC. Альтернативное описание в данном случае удобнее, т. к. оно позволяет более наглядно показать обработку блока остатка с использованием примеров CFB64 из [FIPS-81].

Пакет PDU включает DA, SA и поля тип/длина. В приведенных здесь примерах не предполагалось использовать корректные значения этих полей. В результате, приведенные здесь примеры не являются реальными пакетами, пригодными для передачи. Задача заключалась только в том, чтобы показать на примерах подробности шифрования.

В этих примерах TEK и IV взяты из примера пакета ответа на запрос ключа, описанного выше.

I.7.1 Шифрование только CBC

Когда число октетов, которые предполагают шифровать, кратно 8, используют режим шифрования DES-CBC, как описано в [FIPS-81]. Ключ шифрования и IV пересылают в пакете ответа на запрос ключа.

Здесь рассматривается шифрование DES-CBC с использованием таблицы, в которой показан ключ, IV, вход в незашифрованный текст и выход зашифрованного текста. Для сравнения здесь приведена таблица, в которой описан пример из таблицы C1 [FIPS-81]:

Режим	CBC
Ключ	01 23 45 67 89 ab cd ef
IV	12 34 56 78 90 ab cd ef
Незашифрованный текст	4e 6f 77 20 69 73 20 74 68 65 20 74 69 6d 65 20
Зашифрованный текст	e5 c7 cd de 87 2b f2 7c 43 e9 34 00 8c 38 9c 0f

Представим, что пакет PDU до шифрования выглядит следующим образом:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Тип/Длина	00 01
Пользовательские данные	02 03 04 05 06 07 08 09 0a 0b
CRC	88 41 65 06

Шифрование DES-CBC выполняют следующим образом:

Режим	CBC
Ключ	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Незашифрованный текст	00 01 02 03 04 05 06 07 08 09 0a 0b 88 41 65 06
Зашифрованный текст	0d da 5a cb d0 5e 55 67 9f 04 d1 b6 41 3d 4e ed

Пакет PDU после шифрования выглядит следующим образом:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Тип/Длина	0d da
Пользовательские данные	5a cb d0 5e 55 67 9f 04 d1 b6
CRC	41 3d 4e ed

I.7.2 CBC с обработкой блока остатка

При числе предназначенных для шифрования октетов больше 8 и не кратных 8, режим шифрования является комбинацией DES-CBC и DES-CFB64.

Шифрование начинают в режиме DES-CBC. Режим DES-CBC используют для обработки возможно большего числа представленных законченных блоков DES. Ключ шифрования и IV передают пакетом в ответе на запрос ключа.

После шифрования DES-CBC, имеется от 1 до 7 еще не зашифрованных октетов. Эти октеты шифруют, используя режим DES-CFB64. Режим DES-CFB64 – это "64-битовый режим шифрования с обратной связью", определенный в [FIPS-81]. Ключ шифрования – это пакет ответа на запрос ключа. Обозначение IV – это последние 8 октетов шифрованного текста, созданного обработкой DES-CBC.

Здесь рассматривается шифрование DES-CFB64 с использованием таблицы, в которой показаны ключ, IV, вход в незашифрованный текст и выход зашифрованного текста. Для сравнения здесь приведена таблица, в которой описан пример из таблицы D3 [FIPS-81]:

Режим	CFB64
Ключ	01 23 45 67 89 ab cd ef
IV	12 34 56 78 90 ab cd ef
Незашифрованный текст	4e 6f 77 20 69 73 20 74 68 65 20 74 69 6d 65 20
Зашифрованный текст	f3 09 62 49 c7 f4 6e 51 a6 9e 83 9b 1a 92 f7 84

Представим, что пакет PDU до шифрования выглядит следующим образом:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Тип/Длина	00 01
Пользовательские данные	02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
CRC	91 d2 d1 9f

Всего предполагается зашифровать 19 октетов. Первые 16 октетов обрабатывают, используя метод шифрования DES-CBC, а последние 3 октета – используя шифрование DES-CFB64.

Шифрование DES-CBC выполняют следующим образом:

Режим	CBC
Ключ	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Незашифрованный текст	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 91
Зашифрованный текст	0d da 5a cb d0 5e 55 67 51 47 46 86 8a 71 e5 77

Шифрование DES-CFB64 выполняют следующим образом:

Режим	CFB64
Ключ	e6 60 0f d8 85 2e f5 ab
IV	51 47 46 86 8a 71 e5 77
Незашифрованный текст	d2 d1 9f 00 00 00 00 00
Зашифрованный текст	ef ac 88 e8 ee 80 33 14

Ключ является тем же, который используют для операции шифрования DES-CBC. Значение IV – это последние 8 октетов зашифрованного текста, который генерирует операция DES-CBC.

Отметим, что 5 октетов со значением 0 были присоединены к 3 октетам незашифрованного текста. Значения этих присоединенных октетов не оказывает влияния на значения первых трех зашифрованных октетов, которые являются именно октетами зашифрованного текста, представляющим для нас интерес. Для присоединенных октетов с незашифрованным текстом, вместо 0, можно использовать произвольные значения.

Пакет PDU после шифрования выглядит следующим образом:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Тип/Длина	0d da
Пользовательские данные	5a cb d0 5e 55 67 51 47 46 86 8a 71 e5
CRC	77 ef ac 88

I.7.3 Укороченный кадр

При числе предназначенных для шифрования октетов меньше 8, режим шифрования – это DES-CFB64. Ключ шифрования и IV передают в пакете ответа на запрос ключа.

Представим, что пакет PDU до шифрования выглядит следующим образом:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Тип/Длина	00 01
Пользовательские данные	02
CRC	88 ee 59 7e

Шифрование DES-CFB64 выполняют следующим образом:

Режим	CFB64
Ключ	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Незашифрованный текст	00 01 02 88 ee 59 7e 00
Зашифрованный текст	17 86 a8 03 a0 85 75 01

Отметим, что один октет со значением 0 был присоединен к 7 октетам незашифрованного текста. Значения этого присоединенного октета не оказывает влияния на значения первых семи зашифрованных октетов, которые являются именно октетами зашифрованного текста, представляющим для нас интерес. Для присоединенного октета с незашифрованным текстом, вместо 0, можно использовать произвольные значения.

Пакет PDU после шифрования выглядит следующим образом:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Тип/Длина	17 86
Пользовательские данные	a8
CRC	03 a0 85 75

I.7.4 40-битовый ключ

Протокол BPKM всегда генерирует и распределяет 56-битовые ключи DES. Если требуется 40-битовое шифрование, 56-битовый ключ DES конвертируют вместе с использованием 40-битового ключа, маскируя (до нуля) 16 из 56 битов ключа TEK.

Ключ TEK состоит из 8 октетов. Каждый октет содержит 7 битов ключа и 1 бит проверки четности. Ниже описана процедура конвертирования TEK в 40-битовый ключ:

- первые два октета TEK устанавливают на 0;
- два наиболее значащих битов третьего октета TEK устанавливают на 0;
- оставшиеся пять октетов TEK оставляют неизменными.

Например, если TEK, распределенный по протоколу BPKM, составляет:

ff ff ff ff ff ff ff ff,

то конвертирование 40 битов приводит TEK к виду:

00 00 3f ff ff ff ff ff.

За исключением этого преобразования значения TEK, процедура для 40-битового шифрования пакета PDU идентична процедуре 40-битового шифрования.

Для иллюстрации 40-битового шифрования, предыдущий пример пакета PDU повторен здесь с преобразованием TEK к 40 битам.

Представим, что пакет PDU до шифрования выглядит следующим образом:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Тип/Длина	00 01
Пользовательские данные	02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
CRC	91 d2 d1 9f

Всего предполагается зашифровать 19 октетов. Первые 16 октетов обрабатывают, используя метод шифрования DES-CBC, а последние 3 октета – используя шифрование DES-CFB64.

Шифрование DES-CBC выполняют следующим образом:

Режим	CBC
Ключ	00 00 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Незашифрованный текст	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 91
Зашифрованный текст	44 c8 4a 41 14 67 56 a2 dc 64 8f b0 dc 1e 1e 86

Ключ – это ключ TEK, передаваемый в сообщении ответа на запрос ключа, преобразуют в 40-битовый ключ. IV – это то, что передают в сообщении ответа на запрос ключа.

Шифрование DES-CFB64 выполняют следующим образом:

Режим	CFB64
Ключ	00 00 0f d8 85 2e f5 ab
IV	dc 64 8f b0 dc 1e 1e 86
Незашифрованный текст	d2 d1 9f 00 00 00 00 00
Зашифрованный текст	f1 42 aa a3 e4 9b eb 29

Ключом является тот же ключ, который используют для операции шифрования DES-CBC. IV представляет последние 8 октетов зашифрованного текста, генерируемого операцией DES-CBC.

Пакет PDU после шифрования выглядит следующим образом:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Тип/Длина	44 c8
Пользовательские данные	4a 41 14 67 56 a2 dc 64 8f b0 dc 1e 1e
CRC	86 f1 42 aa

I.8 Шифрование пакета PDU с подавлением заголовка полезной нагрузки

В этих примерах показано, каким образом применяют шифрование к пакету PDU при использовании подавления заголовка полезной нагрузки (PHS). В этих примерах использована полезная нагрузка RTP передачи голоса по протоколу IP (VoIP). В этих примерах не используют точные значения полей пакетов PDU. В результате, приведенные здесь примеры не представляют реальные пакеты, пригодные для передачи. Цель этих примеров заключалась только в том, чтобы показать на примерах подробности шифрования.

I.8.1 Нисходящее направление

Представим, что пакет PDU после операции PHS и до шифрования выглядит следующим образом:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Тип/Длина	21 22 23 24 25 26 27 28 29 2a 2b 2c
Пользовательские данные	31 32 33 34 35 36 37 38 39 3a
CRC	93 86 b3 b9

Операция PHS удаляет поле тип/длина, которое в противном случае было бы включено в заголовок Ethernet/802.3. Пользовательские данные состоят из заголовка RTP и голосовых данных. Шифрование применяют, начиная с первого октета заголовка RTP и заканчивая последним октетом CRC, следующим образом:

Режим	CBC
Ключ	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Незашифрованный текст	21 22 23 24 25 26 27 28 29 2a 2b 2c 31 32 33 34 35 36 37 38 39 3a 93 86
Зашифрованный текст	b4 55 da c8 39 1e 0c ed 15 cf b5 79 0a c3 24 5e cf 0f 52 c0 69 f5 f6 6e

Режим	CFB64
Ключ	e6 60 0f d8 85 2e f5 ab
IV	cf 0f 52 c0 69 f5 f6 6e
Незашифрованный текст	b3 b9 00 00 00 00 00 00
Зашифрованный текст	3e 31 de ea 96 6a 88 6b

После шифрования пакет PDU выглядит следующим образом:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Тип/Длина	b4 55 da c8 39 1e 0c ed 15 cf b5 79
Пользовательские данные	0a c3 24 5e cf 0f 52 c0 69 f5
CRC	f6 6e 3e 31

I.8.2 Восходящее направление

Представим, что пакет PDU после операции PHS и до шифрования выглядит следующим образом:

Заголовок RTP	21 22 23 24 25 26 27 28 29 2a 2b 2c
Голосовые данные	31 32 33 34 35 36 37 38 39 3a
CRC	65 cf fe 89

Операция PHS удаляет поля DA, SA и тип/длина, которые в противном случае были бы включены в заголовок Ethernet/802.3. Пользовательские данные состоят из заголовка RTP и голосовых данных. Первые 12 октетов пользовательских данных не шифруют. Шифрование используют, начиная с первого октета голосовых данных и заканчивая последним октетом CRC, следующим образом:

Режим	CBC
Ключ	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Незашифрованный текст	31 32 33 34 35 36 37 38
Зашифрованный текст	d6 88 87 66 1f 66 04 79

Режим	CFB64
Ключ	e6 60 0f d8 85 2e f5 ab
IV	d6 88 87 66 1f 66 04 79
Незашифрованный текст	39 3a 65 cf fe 89 00 00
Зашифрованный текст	c0 07 20 8e 3b 0b b1 b9

После шифрования пакет PDU выглядит следующим образом:

Заголовок RTP	21 22 23 24 25 26 27 28 29 2a 2b 2c
Голосовые данные	d6 88 87 66 1f 66 04 79 c0 07
CRC	20 8e 3b 0b

I.9 Шифрование фрагментированных пакетов

Если пакет фрагментирован, каждый фрагмент шифруют независимо, используя DES-CBC с обработкой блока остатка. Ключи TEK и IV для каждого фрагмента остаются теми же, что и ключи TEK и IV, которые используют для шифрования не фрагментированных пакетов PDU. Шифруют все октеты фрагмента, включая 12 октетов с адресами Ethernet/802.3 назначения и источника (DA/SA) пакета PDU.

В приведенном здесь примере не используется точные значения полей пакета. В результате, приведенный здесь пример не представляет реальный пакет, пригодный для передачи. Цель этого примера заключалась только в том, чтобы показать подробности шифрования.

В этом примере TEK и IV взяты из описанного выше примера пакета с ответом на запрос ключа.

Представим, что пакет разделен на два фрагмента, следующим образом:

Полезная нагрузка фрагмента 1	01 02 03 04 05 06 f1 f2 f3 f4 f5 f6 00 01 02 03 04 05
CRC фрагмента 1	b4 2b 6d d4

Полезная нагрузка фрагмента 2	06 07 08 09 0a 0b 0c 0d
CRC фрагмента 2	48 34 45 36

Первый фрагмент шифруют, используя DES-CBC и DES-CFB64, следующим образом:

Режим	CBC
Ключ	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Незашифрованный текст	01 02 03 04 05 06 f1 f2 f3 f4 f5 f6 00 01 02 03
Зашифрованный текст	47 41 0f 4f fd 78 47 6e c8 1a 67 4e 26 0c 20 c5

Режим	CFB64
Ключ	e6 60 0f d8 85 2e f5 ab
IV	c8 1a 67 4e 26 0c 20 c5
Незашифрованный текст	04 05 b4 2b 6d d4 00 00
Зашифрованный текст	56 6d 5c 58 2f 56 dc 39

После шифрования первый фрагмент выглядит следующим образом:

Полезная нагрузка фрагмента 1	47 41 0f 4f fd 78 47 6e c8 1a 67 4e 26 0c 20 c5 56 6d
CRC фрагмента 1	5c 58 2f 56

Второй фрагмент шифруют, используя DES-CBC и DES-CFB64, следующим образом:

Режим	CBC
Ключ	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Незашифрованный текст	06 07 08 09 0a 0b 0c 0d
Зашифрованный текст	d8 55 0f 59 9d 19 d9 c6

Режим	CFB64
Ключ	e6 60 0f d8 85 2e f5 ab
IV	d8 55 0f 59 9d 19 d9 c6
Незашифрованный текст	48 34 45 36 00 00 00 00
Зашифрованный текст	b4 5f 3e 95 0e e4 d7 df

После шифрования второй фрагмент выглядит следующим образом:

Полезная нагрузка фрагмента 2	d8 55 0f 59 9d 19 d9 c6
CRC фрагмента 2	b4 5f 3e 95

БИБЛИОГРАФИЯ

[IEEE1] IEEE Standard 802-1990, *IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture*, December 1990.

[RFC1750] EASTLAKE (D.), CROCKER (S.), SCHILLER (J.), *Randomness Recommendations for Security*, *IETF RFC 1750*, December 1994.

[RFC2202] CHENG (P.), GLENN (R.), *Test Cases for HMAC-MD5 and HMAC-SHA-1*, *IETF RFC 2202*, September 1997.

[SCHNEIER] SCHNEIER (B.), *Applied Cryptography*, Second Edition, John Wiley, New York, 1996.

[SET Book 2] *SET, Secure Electronic Transaction Specification* – Book 2: Programmer's Guide, Version 1.0, 31 May 1997.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия B	Средства выражения: определения, символы, классификация
Серия C	Общая статистика электросвязи
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	TMN и техническое обслуживание сетей: международные системы передачи, телефонные, телеграфные, факсимильные и арендованные каналы
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 и взаимосвязь открытых систем
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, 2005 г.