Международный союз электросвязи

МСЭ-R
Сектор радиосвязи МСЭ

Рекомендация МСЭ-R BT.1852-1
(10/2016)

Системы условного доступа для цифрового радиовещания

Серия BT

Радиовещательная служба (телевизионная)

Международный союз электросвязи

Предисловие

Роль Сектора радиосвязи заключается в обеспечении рационального, справедливого, эффективного и экономичного использования радиочастотного спектра всеми службами радиосвязи, включая спутниковые службы, и проведении в неограниченном частотном диапазоне исследований, на основании которых принимаются Рекомендации.

Всемирные и региональные конференции радиосвязи и ассамблеи радиосвязи при поддержке исследовательских комиссий выполняют регламентарную и политическую функции Сектора радиосвязи.

Политика в области прав интеллектуальной собственности (ПИС)

Политика МСЭ-R в области ПИС излагается в общей патентной политике МСЭ-T/МСЭ-R/ИСО/МЭК, упоминаемой в Приложении 1 к Резолюции МСЭ-R 1. Формы, которые владельцам патентов следует использовать для представления патентных заявлений и деклараций о лицензировании, представлены по адресу: http://www.itu.int/ITU-R/go/patents/en, где также содержатся Руководящие принципы по выполнению общей патентной политики МСЭ-T/МСЭ-R/ИСО/МЭК и база данных патентной информации МСЭ-R.

Серии Рекомендаций МСЭ-R

(Представлены также в онлайновой форме по адресу: http://www.itu.int/publ/R-REC/en.)

Серия	Название
BO	Спутниковое радиовещание
BR	Запись для производства, архивирования и воспроизведения; пленки для телевидения
BS	Радиовещательная служба (звуковая)
BT	**Радиовещательная служба (телевизионная)**
F	Фиксированная служба
M	Подвижные службы, служба радиоопределения, любительская служба и относящиеся к ним спутниковые службы
P	Распространение радиоволн
RA	Радиоастрономия
RS	Системы дистанционного зондирования
S	Фиксированная спутниковая служба
SA	Космические применения и метеорология
SF	Совместное использование частот и координация между системами фиксированной спутниковой службы и фиксированной службы
SM	Управление использованием спектра
SNG	Спутниковый сбор новостей
TF	Передача сигналов времени и эталонных частот
V	Словарь и связанные с ним вопросы

Примечание. *– Настоящая Рекомендация МСЭ-R утверждена на английском языке в соответствии с процедурой, изложенной в Резолюции МСЭ-R 1.*

Электронная публикация
Женева, 2018 г.

РЕКОМЕНДАЦИЯ МСЭ-R BT.1852-1

Системы условного доступа для цифрового радиовещания

(Вопрос МСЭ-R 49-1/6)

(2009-2016)

Сфера применения

В настоящей Рекомендации изложены принципы, содействующие развитию эффективных методов условного доступа для цифрового радиовещания с использованием либо транспортных потоков MPEG-2, либо протокола транспортирования медиаданных MPEG (MMTP). В настоящей Рекомендации представлена информация о надежной защите от несанкционированного доступа к услугам радиовещания.

Ключевые слова

Условный доступ, система скремблирования, контроль доступа, защита контента, MPEG-2 TS, MMT

Ассамблея радиосвязи МСЭ,

учитывая,

a) что во многих странах растет потребность в защите радиовещательных программ от несанкционированного приема;

b) что эффективный способ обеспечения такой защиты пакетов транспортного потока MPEG-2, мультиплексированных в соответствии с Рекомендацией МСЭ-T H.222.0, заключаются во внедрении систем радиовещания с условным доступом;

c) что эффективный способ обеспечения такой защиты пакетов MMTP, сформированных на основе Рекомендации МСЭ-R BT.2074, заключаются во внедрении систем радиовещания с условным доступом;

d) что разработаны и эксплуатируются образцы систем с условным доступом для услуг цифрового наземного, цифрового кабельного и цифрового спутникового телевизионного вещания, услуг телевизионного вещания на базе протокола Интернет (IP), а также звуковых и мультимедийных услуг и услуг передачи данных;

e) что существует много примеров реализации систем цифрового радиовещания на базе соответствующих Рекомендаций серий BT и BO, например на базе Рекомендации МСЭ-R BO.1516 по системам спутникового цифрового радиовещания;

f) что желательно ограничить количество разных систем условного доступа и при этом учесть различные требования к ряду услуг радиовещания и систем передачи;

g) что изначальное оснащение приемников возможно большим числом общих элементов условного доступа обеспечит для населения максимальную возможность доступа к защищенным услугам при сниженной стоимости оборудования;

h) что системы условного доступа обеспечивают защиту от несанкционированного доступа, и что владельцам авторских прав, поставщикам программ и поставщикам услуг требуются радиовещательные/распределительные сети, обладающие высокой степенью защиты и позволяющие защищать их программы с помощью управления доступом,

рекомендует,

чтобы системы условного доступа для услуг цифрового радиовещания, осуществляющие защиту либо пакетов транспортного потока MPEG-2, либо пакетов MMTP:

– предоставляли услуги, доступные только для санкционированных приемников;

– совместно использовали как можно больше общих элементов приемника; и

– разрабатывались в соответствии с базовыми принципами, изложенными в Приложении 1.

ПРИМЕЧАНИЕ 1. – Примеры реализаций систем условного доступа для цифрового радиовещания приведены в Приложении 2.

Приложение 1

Базовые принципы разработки систем условного доступа для цифрового радиовещания

1 Введение

Описанные в настоящем Приложении принципы должны способствовать развитию эффективных систем условного доступа, предназначенных для цифрового радиовещания, которые удобны как для абонентов, так и для поставщиков услуг и обеспечивают надежную защиту информации от несанкционированного доступа.

Эти принципы применяются, в основном, к доставке услуг цифрового телевизионного вещания, услуг звукового вещания, а также мультимедийных услуг и услуг передачи данных. Эти принципы применяются к доставке абонентам как соответствующих Рекомендации МСЭ-Т H.220.0 пакетов транспортного потока, так и пакетов MMTP с использованием различных сред передачи, таких как цифровое наземное, цифровое кабельное и цифровое спутниковое радиовещание, а также радиовещание на базе протокола Интернет (IP).

2 Нормативные справочные документы

Рекомендация МСЭ-Т .222.0 | ИСО/МЭК 13818-1: Информационная технология – Общее кодирование подвижных изображений и соответствующей аудиоинформации: Системы

Рекомендация МСЭ-R BT.2074: Конфигурация услуг, протокол транспортирования медиаданных и информация сигнализации для радиовещательных систем на базе MMT

3 Термины, определения и аббревиатуры

3.1 Термины и определения

Скремблирование в цифровом радиовещании

Криптографическое кодирование радиовещательного контента, включающего изображение/звук/данные, с целью предотвращения несанкционированного приема информации в нешифрованном формате. Данное криптографическое кодирование является определяемым процессом, осуществляемым под управлением системы условного доступа (на передающем конце).

Дескремблирование в цифровом радиовещании

Криптографическое декодирование радиовещательного контента, включающего изображение/звук/данные, с целью обеспечения возможности приема информации в нешифрованном формате. Данное криптографическое декодирование является определяемым процессом, осуществляемым под управлением системы условного доступа (на приемном конце).

Условный доступ

Пользователь получает доступ к защищенной услуге путем взаимодействия с использованием функциональной возможности условного доступа, имеющейся в приемнике. Если во время сеанса взаимодействия выполняются все условия доступа, то происходит санкционирование, сообщается ключ для декодирования шифра, и контент восстанавливается.

В результате аутентификации абонента, подтверждения учетной записи и проверки готовности обслуживания или других параметров управления программой активируется сеансовый ключ шифрования/дешифрования, позволяющий сеансу завершить процесс санкционирования.

Управление условным доступом

На передающем конце функция управления условным доступом должна генерировать информацию для управления скремблированием и "ключи" шифрования, относящиеся к услуге.

На приемном конце функция управления условным доступом должна создавать информацию для управления дескремблированием в сочетании с "ключами", относящимися к услуге.

Шифрование и дешифрование

Эти термины используются для обозначения методов, применяемых для защиты (и восприятия) некоторой информации, которая содержится в "сообщениях, связанных с доступом". Эти сообщения должны передаваться от передающего конца на приемный конец функций управления условным доступом.

Пункт отправления

В системе распределения имеется пункт, в котором программы или другой контент первоначально преобразуются в сигнал в своем окончательном формате, предназначенном для радиовещания/распределения. От этого пункта начинается сквозная защита данных. Поступающий на вход контент может иметь любую форму, которая может и не восприниматься человеком. Сам вход контента не должен быть открытым.

ПРИМЕЧАНИЕ 1. – Владельцы авторского права, поставщики услуг и дистрибьюторы формируют большую иерархическую структуру, состоящую из многих возможных пунктов отправления, в рамках поступающего абоненту потока информации, и следовательно, потока скремблированного контента и зашифрованных ключей. Пункт отправления должен начинаться от владельца авторского права или продюсера. На практике большинство пунктов отправления являются просто пунктами входа, при этом каждый из них является уникальным и независимым пунктом, из которого может обеспечиваться устойчивое сопровождение информации на всем пути ее следования до абонента, вне зависимости от ее возможного формата при вводе.

Пункт представления

Последний пункт системы распределения, в котором программы или другой контент представлены в виде сигнала, прежде чем они примут воспринимаемую человеком форму на экране приемника и в громкоговорителях. В этом пункте завершается защита выхода.

Контент

Цифровые данные в любой форме, которые могут быть получены и представлены каким-либо устройством.

Услуга

Один или несколько потоков данных, предназначенных для совместного представления.

Защита услуги

Такая защита услуги, при которой прием и декодирование ее данных возможны только с использованием санкционированных устройств.

3.2 Аббревиатуры

Ks	Scrambling key	Ключ скремблирования
Kw	Work key	Рабочий ключ
Km	Master key	Главный ключ
EMM	Entitlement management message	Сообщение для управления предоставлением прав
ECM	Entitlement control message	Сообщение для управления доступом на основе предоставленных прав
CRC	Cyclic redundancy check	Проверка циклическим избыточным кодом
DES	Data encryption standard	Стандарт шифрования данных
AES	Advanced encryption standard	Усовершенствованный стандарт шифрования
CBC	Cipher block chaining	Сцепление шифрованных блоков
CTR	Counter	Счетное устройство
MAC	Message authentication code	Код аутентификации сообщений
MMT	MPEG media transport	Транспортирование медиаданных MPEG
MMTP	MPEG media transport protocol	Протокол транспортирования медиаданных MPEG
OFB	Output feedback	Обратная связь по выходу
RMP	Rights management and protection	Управление правами и их защита

4 Общее описание системы условного доступа

Существуют две основные функции, входящие в состав системы условного доступа для цифрового радиовещания: скремблирование и контроль доступа. Они являются отдельными и во многих случаях независимыми компонентами системы условного доступа, каждый их которых представляет отдельный информационный процесс.

4.1 Эталонная модель

При условном доступе требуется, чтобы информация *скремблировалась* до ее радиовещательной передачи. Данный процесс осуществляется с использованием криптографического кодирования радиовещательного потока битов.

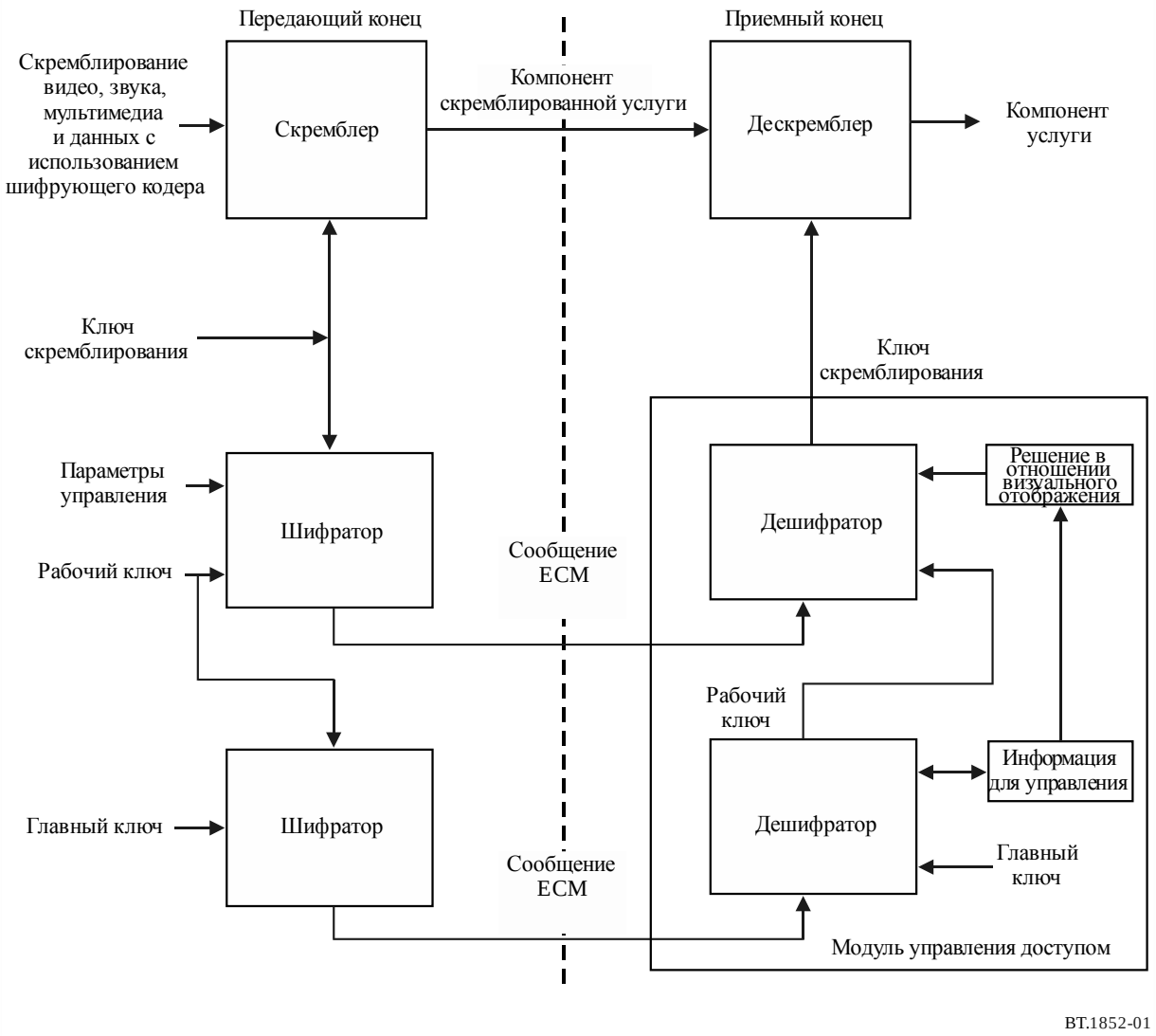
На приемном конце для процесса дескремблирования требуется аналогичное криптографическое декодирование (в данном случае – процедура дескремблирования), чтобы восстановить первоначальный поток битов.

Для выполнения данной последовательности и обеспечения синхронности между процессами отправки и получения, условия криптографического кодирования управляются данными, передаваемыми от шифрующего кодера шифрующему декодеру по специальному протоколу.

Подробная структура данного процесса представлена на рисунке 1.

РИСУНОК 1

Пример блок-схемы системы условного доступа для цифрового радиовещания



4.2 Скремблирование

Процесс защиты некоторых или всех компонентов услуги с целью предотвращения несанкционированного доступа за счет использования криптографического кодирования, осуществляемого на передающем конце, под управлением систем условного доступа.

4.3 Контроль доступа

Предоставление информации, позволяющей санкционированным пользователям дескремблировать сигнал защищаемой услуги. Управление доступностью данной информации осуществляется системой условного доступа.

Между передатчиком и приемником(ами) данная информация группируется в специальные сообщения, которые могут быть мультиплексированы в радиовещательный поток битов, или они могут быть доставлены какими-либо иными способами, например, по линии электросвязи.

На приемном конце(ах) эти сообщения воспринимаются системой условного доступа, для того чтобы обеспечить в санкционированном приемнике управление дескремблированием санкционированных частей из принимаемого потока битов.

5 Требования пользователя

5.1 Устойчивость шифра, используемого скремблером и дескремблером, ко взлому

Шифр, используемый в блоках скремблера и дескремблера, должен пройти тщательные испытания на способность противостоять взлому. Рекомендуется использовать шифры, выбранные из международных стандартов.

5.2 Безопасность

Безопасность системы – это степень трудности, с которой сталкивается несанкционированный пользователь при попытке получить доступ к защищаемой услуге.

– *Дескремблирование сигнала без связи с процессом управления доступом.* Является функцией характера услуг и метода скремблирования. Услуги телевизионного и звукового радиовещания, а также услуги передачи данных с помощью радиовещания будут преимущественно цифровыми, и в связи с этим в них можно будет реализовать процессы скремблирования с высокой степенью защиты.

– *Несанкционированное получение ключа управления доступом.* Является функцией безопасности алгоритмов шифрования ключа.

5.3 Выбор общего или частного алгоритма скремблирования

Доступ предоставляется любому санкционированному пользователю, удовлетворяющему условиям доступа, с использованием общего (универсального) или частного алгоритма скремблирования.

Использование общего алгоритма скремблирования предполагает, что процесс дескремблирования будет общим для всех приемников, основанных на стандартном алгоритме скремблирования, независимо от используемой среды доставки. Это позволит применять более дешевое и гибкое оборудование, а также обеспечит возможность конкуренции за счет реализаций поставщиков услуг.

Использование частного алгоритма скремблирования предполагает, что процесс дескремблирования будет осуществляться только теми приемниками, в которых реализованы конкретные алгоритмы.

5.4 Режимы доступа

В системе условного доступа может поддерживаться ряд режимов доступа, например:

– доступность на период времени (подписка на услугу) – период санкционирования длится от начального и до конечного моментов времени;

– отдельная программа или услуга (покупка передачи) – доступность распространяется на конкретную отдельную услугу, независимо от того, используется ли она полностью или не используется;

– плата за пользование услугой (на основе метки) – плата или использование кредита пропорциональны длительности использования и/или стоимости рассматриваемой услуги;

– открытое вещание – осуществляется защита услуги, однако доступ предоставляется бесплатно.

Необходимо, чтобы имелась возможность регулирования применительно к нескольким параметрам режимов доступа, например:

– времени;

– различным сегментам услуги;

– группам пользователей, которым предназначена услуга.

5.5 Стандартизация оборудования

Для обеспечения максимальной экономии на масштабах производства применительно к приемному оборудованию, а также для упрощения управления и технического обслуживания:

– общее оборудование должно быть стандартизировано, с тем чтобы оно могло использоваться для возможно большего количества услуг;

– требуется, чтобы архитектура абонентского приемника поддерживала требования выбранной системы условного доступа к функциональным возможностям условного доступа. В зависимости от выбранной системы, функциональная возможность может потребовать поддержки встроенной или подключаемой функциональной возможности безопасности (например, смарт-карты).

5.6 Управление доступом

Определение условного доступа базируется на формальном понятии *предоставления прав* на доступ, которое может быть реализовано в различных формах. Предоставление прав дает их обладателю *разрешение* на доступ к связанной с этими правами услуге. Следует предотвращать неэкономное использование ресурсов, обусловленное чрезмерными накладными расходами на управление и передачу.

5.7 Недопущение сбоев в обслуживания

Следует предотвращать сбои, вызванные ошибочным или ненадежным получением данных управления доступом.

6 Сообщения для управления доступом на основе предоставленных прав (ECM)

В сообщениях ECM предоставляются ключи скремблирования, предназначенные для дескремблирования защищаемой услуги.

Доступ по ключу скремблирования в сообщении ECM контролируется с помощью разрешений или прав, предоставляемых в сообщении EMM.

Как правило, сообщения ECM предоставляются в радиовещательном потоке вместе с защищаемой услугой.

Чтобы свести к минимуму ущерб, вызванный утечкой информации о ключе, обычно используется частое изменение ключей скремблирования.

Содержание сообщения ECM зависит от системы.

7 Сообщения для управления предоставлением прав (EMM)

При обработке сообщения для управления предоставлением прав проверяются или предоставляются права, необходимые для дескремблирования защищаемой услуги. В сообщении EMM может содержаться рабочий ключ, обеспечивающий шифрование и дешифрование ключа скремблирования. Сообщения и/или рабочие ключи, предназначенные для отдельных приемников, шифруются. При шифровании может использоваться главный ключ, который может храниться в приемном устройстве.

В системах условного доступа для цифрового радиовещания, сообщения для управления предоставлением прав распределяются с помощью радиовещания или с использованием других сред передачи.

– Распределение с помощью услуг радиовещания называется "адресацией по эфиру". Время цикла, связанного с распределением передаваемых по эфиру ключей, может быть сокращено за счет применения принципов шифрования с использованием разделенного ключа. Распределение сообщений для управления предоставлением прав может также осуществляться по другим средам передачи.

– Распределение по другим средам передачи, как правило, выполняется с использованием соединений пункта с пунктом, обеспечивающих, таким образом, дополнительную меру безопасности, которая гарантирует доступ к сообщению лишь со стороны целевых устройств.

Ниже приводится пример режима работы:

В случае, если платеж осуществляется за единицу времени или за программу, в сообщении для управления может содержаться зашифрованный код цены, передаваемый как часть услуги. Информация о кредите может содержаться в приемнике и приобретать вид шифрованных денежных меток, которые передаются в рамках адресации услуги по эфиру. Другой вариант заключается в том, что кредит может приобретать вид накопленных

денежных меток, распределяемых другими способами. Платеж заключается в уменьшении величины накопленного кредита в соответствии с полученным кодом цены.

Содержание сообщения EMM зависит от системы.

8 Функциональная возможность приемника по управлению доступом

На приемном конце условный доступ может быть осуществлен многими способами, включая следующие:

Тип 1: Функциональная возможность безопасности (которая может включать алгоритм шифрования ключа и главные ключи) и функциональная возможность дескремблирования реализуются в приемнике.

Тип 2: Функциональная возможность безопасности является подключаемой (например, смарт-карта), а функциональная возможность дескремблирования реализуется в приемнике.

Тип 3: Функциональные возможности безопасности и дескремблирования являются подключаемыми; все функции, выполняющие восстановление потока входных данных, реализуются в съемном модуле, взаимодействующем с приемником через стандартный интерфейс (например, общий интерфейс); в этом случае может использоваться любой приемник с таким интерфейсом.

Функциональная возможность безопасности, по запросу, проверяет условия, и если они выполняются, предоставляет дешифратору ключ скремблирования. Эти условия могут включать:

– требование в отношении периода времени, при котором дата, содержащаяся в параметре управления, попадает в интервал между датами начала и окончания действия, указанными в параметре санкционирования;

– требование в отношении цены, при котором санкционирование может быть осуществлено только в том случае, если плата принята модулем безопасности.

В системе условного доступа транзакция может быть реализована с использованием функциональной возможности безопасности, которая включает различные этапы, например:

– предварительные инструкции, если имеются (например, пароль, одобрение пользователя и т. д.);

– рабочие инструкции с использованием модуля безопасности;

– обработка результата (например, доставка слова для скремблирования).

Приложение 2 (для информации)

Примеры реализации системы условного доступа для цифрового радиовещания

ТАБЛИЦА 1

Примеры реализации

Упоминание в Приложении 1	**Система "Роскрипт"**	**Система "CAS-R"**	**"ARIB B61-CAS"**	**Системы стандарта МЭК 62455 с поддержкой DVB**
п. 4. Тип шифра, используемого в скремблере и дескремблере	Основан на государственном стандарте Российской Федерации 28147-89.	MULTI2 (ИСО/МЭК 9979)	– AES (ключ длиной 128 битов) (ИСО/МЭК 18033-3) – Camellia (ключ длиной 128 битов) (ИСО/МЭК 18033-3)	DVB-CSA или AES-128 (обязателен для устройств); также возможно использование DES, 3DES и MULTI2 (не обязательны для устройств)
п. 4. Процесс скремблирования	Циклическое многошаговое преобразование на основе регистров сдвига с использованием полиномов 64-й степени. Основан на нелинейных алгоритмах и является практически случайной последовательностью (не имеет аналитического выражения).	a) Для 64-битовых кодированных последовательностей, исходное кодирование заменяется другой двоичной кодовой последовательностью, использующей переменные длиной 64 и 256 битов. b) Для кодовых последовательностей с длиной менее 64-х битов, описанный в пункте a), выше, метод используется для генерации серии псевдослучайных кодированных последовательностей, которые объединяются для создания скремблированного сигнала.	– Для пакетов MPEG-2 TS, режим CBC+OFB – Для пакетов MMTP, режим CTR	DVB-CSA: согласно ETSI ETR-289; AES-128: согласно FIPS PUB 197:2001, с использованием режима ECB или CBC; DES или 3DES: согласно FIPS PUB 46-3:1999 и FIPS PUB 81:1980; MULTI2 согласно ИСО/МЭК 9979
п. 4. Синхронизация и процесс скремблирования	Взаимная синхронизация схем формирования случайной последовательности и потока DVB.	Для синхронизации процесса скремблирования используется сопутствующая информация, содержащаяся в сообщениях ECM (информация о программе и информация для управления), EMM (информация об отдельных абонентах), общих сообщениях EMM и индивидуальных сообщениях EMM.	Для синхронизации процесса скремблирования используется сопутствующая информация, содержащаяся в сообщениях ECM (информация о программе и информация для управления), EMM (информация об отдельных абонентах), общих сообщениях EMM и индивидуальных сообщениях EMM	Для облегчения синхронизации в сообщение ключевого потока, в котором доставляется ключ шифрования трафика, включаются поля odd_even_flag (признак четного/нечетного ключа) и initial_vector (начальный вектор). Соответствующие значения битов поля transport_scrambling_control (управление скремблированием транспортного потока) указывают на то, какой ключ должен использоваться в данный момент времени.

ТАБЛИЦА 1 (*продолжение*)

Упоминание в Приложении 1	**Система "Роскрипт"**	**Система "CAS-R"**	**"ARIB B61-CAS"**	**Системы стандарта МЭК 62455 с поддержкой DVB**
п. 6. Сообщения для управления доступом на основе предоставленных прав (ECM)	Содержание сообщения ECM: – идентификатор рабочего ключа; – ключ скремблирования (четный/нечетный); – зашифрованный счетчик и криптографическая контрольная сумма. Используются структурная избыточность потока DVB или дополнительно присваиваемые резервы.	Раздел ECM и основная архитектура информационного содержания сообщения ECM: – для всего раздела ECM применяется раздел CRC; – информационное содержание ECM состоит из фиксированной части, которая передается всегда, и переменной части, содержание которой меняется в зависимости от цели передачи; – в переменную часть сообщения ECM включается только необходимая информация для функции ECM.	Раздел ECM и основная архитектура информационного содержания сообщения ECM: – для всего раздела ECM применяется раздел CRC; – информационное содержание ECM состоит из фиксированной части, которая передается всегда, и переменной части, содержание которой меняется в зависимости от цели передачи; – в переменную часть сообщения ECM включается только необходимая информация для функции ECM.	В ECM передается сообщение ключевого потока, которое содержит поля для передачи следующей информации: – content_key_index (индекс ключа контента); – odd_even_flag (признак четного/нечетного ключа); – cipher mode (режим шифрования); – next_initial_vector (следующий начальный вектор); – encrypted_traffic_key_material (материал ключа шифрованного трафика); – traffic_key_lifetime (продолжительность действия ключа трафика); – timestamp (метка времени); – access_criteria_descriptors (дескрипторы критериев доступа); – permissions_category (категория разрешений); – encrypted_programme encryption key (зашифрованный ключ шифрования программы); – programme_CID_extension (CID-расширение программы); – programme_MAC (MAC-код программы); – service_CID_extension (CID-расширение услуги); – service_MAC (MAC-код услуги). Включение этих полей в конкретное сообщение ключевого потока зависит от ряда факторов, например, от того, хочет ли поставщик услуг разрешить доступ для каждой отдельной программы.

ТАБЛИЦА 1 (*продолжение*)

Упоминание в Приложении 1	**Система "Роскрипт"**	**Система "CAS-R"**	**"ARIB B61-CAS"**	**Системы стандарта МЭК 62455 с поддержкой DVB**
Главный ключ	256 битов	Длина главного ключа зависит от оператора услуги.	Длина главного ключа зависит от оператора услуги.	"Главный ключ" как таковой отсутствует. Защита ключей шифрования услуги (SEK) или ключей шифрования программы (PEK) основана на ключах RSA длиной 1024, 2048 или 4096 битов, в зависимости от доверительного центра. В режиме радиовещания аналогичную роль играет 128-битовый предполагаемый ключ шифрования (IEK). Он выводится из набора ключей, которые доставляются в приемник во время регистрации. Защита этого набора ключей основана на ключах RSA длиной 1024, 2048 или 4096 битов.
п. 6. Изменение ключа и признак скремблирования	Ключ скремблирования меняется по мере необходимости. Используются все четыре состояния признака.	Ключи скремблирования (четный/нечетный) меняются как правило каждые две секунды.	Ключи скремблирования (четный/нечетный) меняются с интервалом более одной секунды.	Ключ шифрования трафика меняется часто – от одного раза в минуту до одного раза в секунду.

ТАБЛИЦА 1 (*продолжение*)

Упоминание в Приложении 1	**Система "Роскрипт"**	**Система "CAS-R"**	**"ARIB B61-CAS"**	**Системы стандарта МЭК 62455 с поддержкой DVB**
п. 7. Сообщения для управления предоставлением прав (EMM)	Содержание сообщения EMM: – номер протокола; – идентификатор группы радиовещательной организации; – рабочий ключ; – идентификатор программы; – идентификатор модуля безопасности; – права доступа; – зашифрованный счетчик и криптографическая контрольная сумма. используются структурная избыточность потока DVB или дополнительно присваиваемые резервы.	В разделе EMM может передаваться множественное информационное содержание. – Для всего раздела EMM применяется обнаружение ошибок методом CRC. – Информационное содержание EMM состоит из фиксированной части, которая передается всегда, и переменной части, содержание которой меняется в зависимости от цели передачи. – В переменную часть сообщения EMM включается только необходимая информация для функции EMM. Идентификатор карты (6 байтов) и сопутствующая информация длиной 1 байт передаются в начале фиксированной части EMM (нешифрованная часть). Приемник отфильтровывает эту область, чтобы идентифицировать адресованное ему информационное содержание.	В разделе EMM может передаваться множественное информационное содержание. – Для всего раздела EMM применяется обнаружение ошибок методом CRC. – Информационное содержание EMM состоит из фиксированной части, которая передается всегда, и переменной части, содержание которой меняется в зависимости от цели передачи. – В переменную часть сообщения EMM включается только необходимая информация для функции EMM. Идентификатор устройства (8 байтов) в случае RMP или идентификатор модуля (6 байтов) в случае CAS и сопутствующая информация длиной 1 байт передаются в начале фиксированной части EMM (нешифрованная часть). Приемник отфильтровывает эту область, чтобы идентифицировать адресованное ему информационное содержание.	В интерактивном режиме, для доставки в приемники прав, а также ключей шифрования услуги (SEK) или ключей шифрования программы (PEK), вместо сообщений для управления предоставлением прав используются объекты прав OMA DRM 2.0. Эти права доставляются по интерактивным каналам. В режиме радиовещания используется специальная двоичная версия этих объектов прав под названием BCRO.
п. 8. Функциональная возможность управления доступом	Расположена в модуле условного доступа (CAM) или встроена в абонентскую приставку (STB).	Тип 2: Модуль безопасности является съемным, а модуль дескремблирования встроен в приемник.	Тип 1: Модули безопасности и дескремблирования реализованы в приемнике. Тип 2: Модуль безопасности является съемным, а модуль дескремблирования встроен в приемник.	Предполагается использование типа 1, однако также не исключаются другие реализации.

ТАБЛИЦА 1 (*окончание*)

Упоминание в Приложении 1	**Система "Роскрипт"**	**Система "CAS-R"**	**"ARIB B61-CAS"**	**Системы стандарта МЭК 62455 с поддержкой DVB**
Зашифрованный счетчик и криптографическая контрольная сумма	ECM и EMM	Код MAC (код аутентификации сообщения) включается как в пакеты ECM, так и в пакеты EMM	Код MAC (код аутентификации сообщения) включается как в ECM, так и в EMM. Код MAC может быть также добавлен к каждому пакету MMTP.	Код MAC (код аутентификации сообщения) включается в сообщения ключевого потока и в объекты прав, используемые в режиме радиовещания. В интерактивном режиме объекты прав защищаются с помощью подписи.
п. 8. Функциональная возможность безопасности	Расположена в модуле условного доступа (CAM) или встроена в абонентскую приставку (STB)	Взаимно аутентифицируется смарт-картой и приемником.	Взаимно аутентифицируется смарт-картой и приемником для типа 1 и типа 2. В случае Типа 1 безопасность системы контроля доступа можно обеспечиваться и совершенствоваться путем ее загрузки и обновления.	Стандарт не определяет реализацию. Правила соответствия и устойчивости устанавливаются доверительным центром.

1 Описание системы "Роскрипт"

В настоящее время система условного доступа (СУД) "Роскрипт" внедряется в России в связи с переходом на цифровое телевизионное радиовещание. Система "Роскрипт" предназначена для защиты потоков данных DVB от несанкционированного приема. Система обладает широким диапазоном использования с различными цепочками спутникового и наземного радиовещания в формате DVB и гибкостью в управлении своей абонентской базой.

В состав системы "Роскрипт" входят:

- *скремблер*, который выполняет шифрование предварительно выбранных компонентов транспортного потока DVB; он может работать автономно и под управлением компьютера;
- *модуль CAM*, предназначенный для дескремблирования выбранных компонентов, который вставляется в разъем общего интерфейса в приемнике (ОИ);
- *модуль безопасности*, имеющий встроенную абонентскую приставку.

Оборудование, необходимое для работы общей системы управления и мониторинга, установлено на передающем конце.

Система "Роскрипт" решает следующие задачи:

- ограничение радиовещания территорией страны для защиты прав владельцев программ на ограниченное радиовещание;
- защита корпоративных и ведомственных систем радиовещания от несанкционированного доступа;
- организация коммерческого радиовещания.

В системе "Роскрипт" учитываются характерные особенности цепочек, защищаемых от несанкционированного доступа.

1.1 Функциональные и технические характеристики системы "Роскрипт"

- Общая модель работы СУД "Роскрипт" соответствует рисунку 1 в Приложении 1.
- *Алгоритм скремблирования*: Имеются два частных алгоритма скремблирования, которые реализованы в скремблере и дескремблере СУД "Роскрипт". Оператор может в любой момент поменять текущий алгоритм скремблирования.
- *Ключи безопасности*: В системе "Роскрипт" используются следующие ключи:
  - Ключ скремблирования и рабочий ключ обеспечивают скремблирование/дескремблирование контента.
  - База однозначно определяемых главных ключей обеспечивает дешифрование сообщения ECM (рабочий ключ) и управление доступом со стороны абонента.
  - Группа ключей программы позволяет отделять абонентов разных операторов друг от друга и классифицировать всех абонентов по любому критерию.
  - Операторы могут быстро менять ключи, не прибегая к физическому и электронному распределению.
- *Режим доступа*: Существует два режима доступа, позволяющих эффективно управлять абонентской базой: доступность на период времени и отдельная программа и услуга.
  - параметры режима доступа: скорость управления абонентской базой составляет 1000 абонентов в секунду; количество абонентов не ограничено; количество компонентов скремблирования равно 150; количество групп пользователей – 64 000.

– *EMM и ECM*: Структура сигналов EMM и ECM соответствует пп. 6 и 7 Приложения 1.

  – В конце каждого пакета EMM и ECM находится зашифрованный счетчик и криптографическая контрольная сумма.

  – Для доставки команд управления (EMM и ECM) могут использоваться как дополнительные ресурсы в ширине полосы потока DVB, так и резервы структурной скорости (структурная избыточность) транспортного потока DVB.

– *Приемное оборудование*: На приемной стороне возможно использование двух типов систем условного доступа "Роскрипт":

  – модуль безопасности, который включает алгоритм шифрования ключа для ключей безопасности и модуль дескремблирования, встроен в абонентскую приставку.

  – модуль условного доступа (CAM), который включает модули безопасности и дескремблирования и взаимодействуют с приемником через стандартный общий интерфейс (ОИ), является съемным. Один модуль CAM может одновременно восстанавливать скремблированные компоненты входного транспортного потока.

1.2 Другие характеристики

– Один комплект передающего оборудования "Роскрипт" может шифровать контент, поступающий от нескольких независимых поставщиков. Данное свойство используется для крупных операторов спутникового и наземного радиовещания.

– Общая система управления и мониторинга позволяет управлять доступом абонента к контенту.

– Общая система управления и мониторинга обеспечивает удаленную централизованную эксплуатацию и мониторинг комплекта передающего оборудования "Роскрипт" на всей сети. Данное свойство используется для крупных операторов спутникового и наземного радиовещания.

2 Описание системы "CAS-R"

2.1 Назначение системы

В стандарте ARIB STD-B25 рассматривается система управления условным доступом, предназначенная для использования в цифровом радиовещании. Определяются спецификации скремблирования и сопутствующей информации, а также соответствующие спецификации приема для системы, которая обеспечивает управление во время приема сигнала (именуемой в дальнейшем "CAS-R").

Настоящим стандартом определяются системы CAS, предназначенные для систем наземного и спутникового цифрового радиовещания, которые в настоящее время используются в Японии.

2.2 Требования к CAS-R и ее делиберативным системам

В стандарте ARIB STD-B25 определяются системы CAS, удовлетворяющие следующим требованиям:

1 Максимальное количество абонентов:

Система может быть расширена для предоставления функций управления абонентами во всех домашних хозяйствах в зоне охвата.

2 Срок службы системы:

Система может управляться за счет поддержки соответствующих вещательных СМИ.

3 Противодействие пиратству:

Система обеспечивает усовершенствованные функциональные возможности безопасности и может принимать меры в случае атак на безопасность.

4 Эти системы применимы ко всем системам цифрового радиовещания в конкретном районе.

5 Способы приема:

a) Прием в реальном времени, включая прием потокового аудио/видео и данных, передаваемых с помощью радиовещания, с использованием формата файла (CAS-R).

b) Прием с накоплением (прием не в реальном времени).

c) Прием с записью (включая резервный прием).

6 Система может использоваться со следующей структурой оплаты: единая/ступенчатая ставка, плата за просмотр (интерактивная плата за просмотр (IPPV)) и бесплатный просмотр.

2.3 Требования к модулю безопасности

1 Шифрование сопутствующей информации:

В системе шифрования используется трехуровневая архитектура с ключами, соответствующими формату DES, и частными ключами. С точки зрения реализации на основе смарт-карты, система шифрования должна иметь небольшой размер программы и позволять высокоскоростную обработку данных с использованием по меньшей мере 8-битового микроконтроллера.

2 Функциональная возможность администрирования:

Система может менять протокол шифрования в целях противодействия пиратству.

3 Между смарт-картой и приемником должна осуществляться взаимная аутентификация:

Если в приложениях, использующих данную систему условного доступа как технологию защиты авторских прав в цифровом радиовещании, для исключения приемников, которые не отвечают на информации о защите прав, применяется смарт-карта типа CAS, то в системе предусматривается взаимная аутентификация между данной смарт-картой и приемником.

2.4 Подробное описание этой системы представлено в следующем документе

Спецификации системы условного доступа ARIB STD B-25 размещены по адресу: http://www.arib.or.jp/english/html/overview/doc/6-STD-B25v5_0-E1.pdf.

3 Описание CAS второго поколения (ARIB B61-CAS) на базе ARIB STD-B61

3.1 Характеристики системы

В ARIB STD-B61 определены система скремблирования, система защиты контента и система загрузки программ CAS для цифрового радиовещания как CAS второго поколения. CAS второго поколения имеет следующие характеристики:

– поддерживает как MPEG-2 TS, так и MMT в качестве базового протокола транспортирования медиаданных;

– поддерживает AES и Camellia длиной 128 байтов в качестве алгоритма шифрования;

– поддерживает безопасную передачу сопутствующей информации;

– обладает возможность поддерживать и повышать уровень безопасности системы контроля доступа с помощью механизма загрузки программ CAS.

3.2 Требования, предъявляемые к системе

1 Требования к подсистеме скремблирования:

– эта подсистема обеспечивает усовершенствованную функциональность безопасности и может принимать меры в случае попыток несанкционированного доступа.

2 Требования к подсистеме сопутствующей информации:

- сопутствующая информация в максимально возможной степени представляется в общем формате;
- предусмотрена возможность передачи информации, предназначенной для отдельных приемников;
- существует возможность безопасной передачи сопутствующей информации;
- существует возможность обеспечения и повышения безопасности на постоянной основе.

3.3 Подсистема скремблирования

В подсистеме скремблирования для поддержания высокого уровня безопасности системы отобраны два алгоритма шифрования: AES или Camellia длиной 128 байтов. Оба алгоритма используются как для пакетов MMTP, так и пакетов MPEG-2 TS.

В случае MPEG-2 TS единицей скремблирования является пакет MPEG-2 TS, исключая заголовок пакета. Поскольку пакет MPEG-2 TS представляет собой пакет фиксированной длины, режимы сцепления шифрованных блоков (CBC) и режим обратной связи по выходу (OFB) используются вместе в качестве режима работы алгоритма шифрования. Алгоритм шифрования определяется идентификатором Scramble_system_id в дескрипторе скремблирования, который является одним из элементов служебной информации.

В случае MMT единицей скремблирования является пакет MMTP, исключая заголовок пакета. Ввиду того, что пакет MMTP имеет переменную длину и относительно большой размер, в качестве режима работы алгоритма шифрования используется режим счетчика (CTR). Алгоритм шифрования определяется идентификатором Scramble_system_id в дескрипторе скремблирования, который является одним из элементов информации сигнализации. Информация для управления скремблированием размещается в поле расширения заголовка пакета MMTP с целью определения следующих трех параметров скремблирования: нешифрованное информационное содержание; информационное содержание, скремблированное с использованием "четного" ключа; и информационное содержание, скремблированное с использованием "нечетного" ключа.

3.4 Подсистема сопутствующей информации

Существует два типа контроля приема сигнала: CAS и система защиты контента. Для каждой системы существует собственная сопутствующая информация.

В CAS второго поколения включена система защиты контента, которая называется "Управление правами и их защита (RMP)", для услуг открытого вещания наряду с контролем приема сигнала. Система RMP обеспечивает для радиовещательных компаний возможность предоставлять каждому приемнику ключ скремблирования, который используется для дешифрования контента.

Притом что система RMP в целом аналогична системе, предназначенной для системы CAS-R, которая упоминалась выше, она может применяться как в случае MMT, так и в случае MPEG-2 TS.

3.5 Трехуровневая архитектура и ECM/EMM

Для CAS второго поколения используется трехуровневая архитектура, а также ECM/EMM, описанные в эталонной модели.

В случае MPEG-2 TS: в сообщении ECM содержится общая информация, предназначенная для всех приемников. Ключ скремблирования передается в сообщении ECM. Доступ по ключу скремблирования в сообщении ECM контролируется с помощью разрешений и прав, предоставляемых в сообщении EMM. В сообщении EMM содержится информация, предназначенная для отдельных приемников. Рабочий ключ передается в сообщении EMM.

В случае MMT: в сообщении ECM содержится общая информация, предназначенная для всех приемников. Ключ скремблирования передается в ECM. Доступ по ключу скремблирования в сообщении ECM контролируется с помощью разрешений и прав, предоставляемых в сообщении EMM. В сообщении EMM содержится информация, предназначенная для отдельных приемников.

Рабочий ключ передается в сообщении EMM. ECM и EMM передаются в сообщении секции M2, которое определено в Рекомендации МСЭ-R BT.2074. Для того чтобы приемник имел возможность проверить целостность и аутентичность пакета, к каждому пакету MMTP может быть добавлен код аутентификации сообщения (MAC).

3.6 Загружаемая CAS

CAS второго поколения включает загружаемую CAS, цель которой – обеспечивать на постоянной основе безопасность системы контроля доступа и поддержку новых радиовещательных услуг. Приемник может осуществлять безопасную загрузку обновленной программы CAS в режиме широковещательной передачи и/или широкополосной связи.

Для загрузки программы CAS по каналам широковещательной передачи используются трехуровневая структура ключей и скремблирование. В каналах широковещательной передачи программа CAS шифруется с помощью ключа защиты канала передачи (Kt), который распределяется каждому приемнику путем направления сообщения для контроля загрузки (DCM) и сообщения для управления загрузкой (DMM).

Программа CAS наряду с шифрованием подписывается своим поставщиком для обеспечения целостности и аутентичности.

4 Описание систем стандарта МЭК 62455 с поддержкой DVB

В стандарте МЭК 62455 определяется стандартизированная система управления доступом к услугам радиовещания на базе транспортного потока MPEG-2. В этом стандарте также определяется то, как так же самая система может использоваться для управления доступом к услугам радиовещания на базе протокола Интернет (IP). Таким образом, эта спецификация может широко применяться к различным системам радиовещания, включая системы, в которых защита не может быть выполнена в пакетах транспортного потока MPEG-2 (например, в услугах на базе IP, доставляемых по сетям, базирующимся на потоке, отличном от MPEG-2).

Для систем радиовещания с условным доступом стандарт МЭК 62455 обеспечивает полностью определенный интерфейс между передающим и приемным концами. Используя этот полностью определенный интерфейс, поставщики серверов и приемников могут независимо реализовывать поддержку системы защиты. При этом им нет нужды полагаться на одного поставщика безопасности, чтобы облегчить реализацию как на стороне сервера, так и на стороне приемника. Таким образом, при реализации системы предотвращается привязка к поставщику безопасности и обеспечивается возможность изменения поставщика любого определенного элемента системы условного доступа, не меняя другие элементы или их поставщиков.

В спецификации МЭК 62455 охватываются все нижеследующие уровни системы, и, по возможности, делаются ссылки на существующие спецификации:

- уровень регистрации;
- уровень управления правами;
- уровень ключевого потока;
- уровень трафика.

Уровень управления правами базируется на устоявшемся и общепринятом в коммерческих кругах стандарте управления цифровыми правами OMA DRM 2.0, разработанном альянсом OMA (Open Mobile Alliance). Данный уровень отвечает за доставку в приемники прав и соответствующих ограничений, а также ключей долговременного пользования, т. е. ключа шифрования услуги (SEK) или ключа шифрования программы (PEK), в зависимости от того, на какой основе предоставляется доступ: на основе подписки или к отдельным программам.

В интерактивном режиме, т. е. когда между приемником и поставщиком услуги имеется двусторонний канал связи, стандарт OMA DRM 2.0 используется сам по себе. При работе однонаправленном вещательном режиме, при отсутствии интерактивного канала, система усовершенствована с помощью двоичных версий объектов прав OMA DRM 2.0 с сокращенной

шириной полосы (называемых двоично-кодированными объектами прав, или BCRO), а также метода защиты этих объектов BCRO при доставке по радиовещательным каналам. Адресация объектов BCRO включает различные режимы, которые еще больше сокращают ширину полосы, необходимую для распределения этих объектов прав. Метод защиты основан на шифровании радиовещательного потока с использованием нулевого сообщения, которое гарантирует, что при нарушении защиты одного приемника не будет обеспечен доступ к ключам для прав, доставляемых в любые другие приемники. Ширина полосы для радиовещания используется весьма оптимально.

Набор ключей, необходимых для работы в режиме радиовещания, доставляется в приемник по радиовещательным каналам во время регистрации для предоставления услуги. Для того чтобы зарегистрироваться для предоставления услуги, пользователю необходимо лишь сообщить уникальный номер устройства (UDN), принадлежащий приемнику, поставщику услуги, который далее может осуществить поиск сертификата приемника в базе данных сертификатов. Этот сертификат содержит открытые ключи приемника, которые используются для защиты набора ключей в процессе транзита.

Чтобы защитить транспортный поток MPEG-2, при шифровании (скремблировании) фактического контента услуги используются распространенные шифры, например DVB-CSA или AES-128, как определено в МЭК 62455. В целях содействия защите транспортного потока, базирующегося на пакетах, отличных от MPEG-2, этим стандартом также определяется поддержка других стандартов шифрования, например IPsec, SRTP и ISMAcryp.

Для облегчения частого изменения ключей шифрования трафика (TEK), используемых для защиты контента услуги, в МЭК 62455 определяется уровень ключевого потока, который работает между уровнем управления правами и уровнем трафика. С помощью объектов прав услуги и программы в системе поддерживается предоставление доступа к тому же потоку. Если поставщик услуги желает разрешить доступ для каждой отдельной программы, когда эта программа также доступна по подписке, то в сообщении ключевого потока будет передаваться ключ PEK, зашифрованный ключом SEK, наряду с ключом TEK, зашифрованным ключом PEK. На уровне ключевого потока может также передаваться другая информация, например, критерии доступа или значение поля permissions_category, которое может использоваться для выбора между различными правами в объекте прав услуги, относящимися к конкретному фрагменту потока, к которому применяется сообщение ключевого потока. Это делает возможным наличие разных прав для разных программ, даже если доступ осуществляется на базе подписки на услугу, содержащую много последовательных программ.

Прилагаемый документ 1 к Приложению 2

Библиография

– Рекомендация МСЭ-R BT.81: Системы радиовещания с условным доступом
– ARIB STD-B25: Спецификации системы цифрового радиовещания с условным доступом
– ARIB STD-B61: Спецификации системы цифрового радиовещания с условным доступом (второго поколения) и системы загрузки программ CAS для цифрового радиовещания
– IEC 62455: Доступ к услуге на основе протокола Интернет (IP) и транспортного потока (TS)