

**ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,  
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ****(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ**(21)(22) Заявка: **2008104858/08**, **10.08.2006**(24) Дата начала отсчета срока действия патента:  
**10.08.2006**

Приоритет(ы):

(30) Конвенционный приоритет:  
**11.08.2005 US 11/201,751**(43) Дата публикации заявки: **20.08.2009** Бюл. № 23(45) Опубликовано: **27.08.2011** Бюл. № 24(56) Список документов, цитированных в отчете о  
поиске: **RU 2002105505 A**, **10.09.2003. US**  
**2004/0243808 A1**, **02.12.2004. US 2004/0049694**  
**A1**, **11.03.2004. WO 2004/030364 A1**, **08.04.2004.**  
**WO 2004/023717 A2**, **18.03.2004.**(85) Дата начала рассмотрения заявки РСТ на  
национальной фазе: **08.02.2008**(86) Заявка РСТ:  
**US 2006/031185 (10.08.2006)**(87) Публикация заявки РСТ:  
**WO 2007/021830 (22.02.2007)**

Адрес для переписки:

**129090, Москва, ул. Б.Спасская, 25, стр.3,  
ООО "Юридическая фирма Городисский и  
Партнеры", пат.пов. Ю.Д.Кузнецову,  
рег.№ 595**

(72) Автор(ы):

**КЛЕМЕТС Андерс Э. (US),  
АЛКОУВ Джеймс М. (US),  
БХАТТ Санджай (US),  
ОЛИВЕЙРА Эдуарду П. (US),  
ПАКА Ананд (US)**

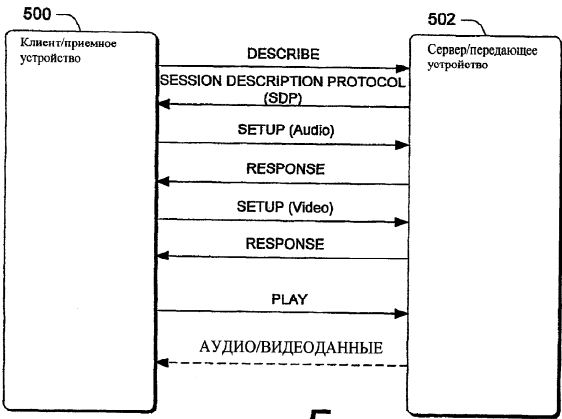
(73) Патентообладатель(и):

**МАЙКРОСОФТ КОРПОРЕЙШН (US)****(54) ЗАЩИТА ЦИФРОВОГО МУЛЬТИМЕДИА С РАЗЛИЧНЫМИ ТИПАМИ СОДЕРЖИМОГО**

(57) Реферат:

Изобретение относится к области DRM-методик защиты цифрового мультимедиа с различными типами контента. Техническим результатом является обеспечение защиты цифрового мультимедиа за счет добавления дескрипторов к каждому из зашифрованных сегментов данных. Способ содержит: формирование корневого ключа содержимого с использованием открытого ключа компьютера клиента-приемника, передачу

корневого ключа содержимого на компьютер клиент-приемник зашифровывают сегменты данных мультимедийного файла, чтобы предоставить зашифрованные сегменты данных, причем каждый сегмент данных зашифрован посредством соответствующего листового ключа содержимого; и добавляют дескрипторы к каждому из зашифрованных сегментов данных, причем каждый из дескрипторов зашифрованных сегментов данных идентифицирует листовой ключ



Фиг. 5

RU 2 4 2 7 8 9 8 C 2

RU 2 4 2 7 8 9 8 C 2



FEDERAL SERVICE  
FOR INTELLECTUAL PROPERTY,  
PATENTS AND TRADEMARKS

(51) Int. Cl.

*G06F 17/00* (2006.01)*H04L 9/00* (2006.01)**(12) ABSTRACT OF INVENTION**(21)(22) Application: **2008104858/08, 10.08.2006**(24) Effective date for property rights:  
**10.08.2006**

Priority:

(30) Priority:  
**11.08.2005 US 11/201,751**(43) Application published: **20.08.2009 Bull. 23**(45) Date of publication: **27.08.2011 Bull. 24**(85) Commencement of national phase: **08.02.2008**(86) PCT application:  
**US 2006/031185 (10.08.2006)**(87) PCT publication:  
**WO 2007/021830 (22.02.2007)**

Mail address:

**129090, Moskva, ul. B.Spasskaja, 25, str.3, OOO  
"Juridicheskaja firma Gorodisskij i Partnery",  
pat.pov. Ju.D.Kuznetsovu, reg.№ 595**

(72) Inventor(s):

**KLEMETS Anders Eh. (US),  
ALKOUV Dzhejms M. (US),  
BKhATT Sandzhaj (US),  
OLIVEJRA Ehduardu P. (US),  
PAKA Anand (US)**

(73) Proprietor(s):

**MAJKROSOFT KORPOREJShN (US)****(54) PROTECTION OF DIGITAL MULTIMEDIA WITH VARIOUS TYPES OF CONTENT**

(57) Abstract:

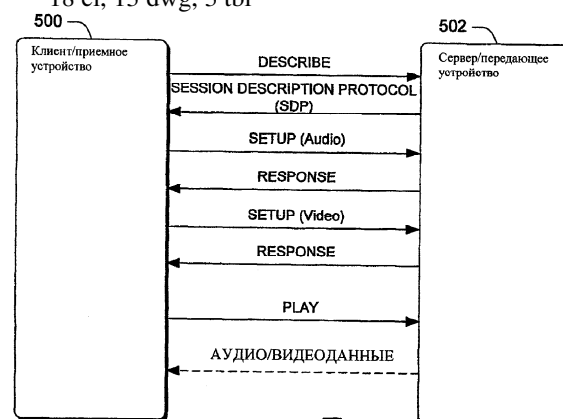
FIELD: information technologies.

SUBSTANCE: method includes the following: generation of a root content key with application of an open key of a computer at a receiving client, transfer of the root content key to a computer of a receiving client. data segments of multimedia file are coded, to provide coded data segments, besides, each data segment is coded by means of an appropriate sheet key of content; and descriptors are added to each of coded data segments, besides, each of descriptors of coded data segments identifies a sheet content key.

EFFECT: provision of digital multimedia protection by addition of descriptors to each of

coded data segments.

18 cl, 13 dwg, 3 tbl



Фиг. 5

### **Уровень техники**

Управление цифровыми правами (DRM) означает методики, которые используются для того, чтобы защищать содержимое, например, посредством контроля или ограничения использования цифрового мультимедийного содержимого в электронных устройствах. Одна характеристика DRM заключается в том, что оно может привязывать мультимедийное содержимое к данной машине или устройству. Таким образом, лицензия, которая относится к конкретному фрагменту содержимого и которая задает права и ограничения, ассоциативно связанные с фрагментом содержимого, типично должна быть привязана к данной машине или устройству. Как результат, пользователь не может брать фрагмент содержимого и перемещать его на другую машину, чтобы воспроизводить содержимое.

Текущие DRM-методики имеют ограничения. Зачастую они совместимы только с двумя типами протоколов для передачи цифрового мультимедиа - HTTP и RTSP. Но другие протоколы сегодня или в будущем могут более оптимально подходить для передачи цифрового мультимедиа. Кроме того, содержимое, защищенное посредством DRM, может быть ограничено конкретным типом содержимого. Один конкретный тип содержимого - ASF-файлы - предоставляет возможность только одному набору прав и ограничений, т.е. политик, применяться ко всему ASF-файлу. Например, когда видео подготавливается посредством рендеринга, может потребоваться либо активировать Macrovision на аналоговом видеовыходе для всего файла, либо он может не потребоваться вообще.

### **Сущность изобретения**

Описаны системы и/или способы ("средства"), которые дают возможность ассоциативно связывать политику управления цифровыми правами с цифровым мультимедиа, имеющим произвольный тип содержимого или протокол управления передачей. В некоторых вариантах осуществления средства шифруют сегменты данных мультимедийного файла и добавляют дескриптор в каждый из этих сегментов. Эти дескрипторы могут предоставлять возможность приемному устройству зашифрованного мультимедийного файла расшифровывать файл и потреблять его согласно корректной политике управления цифровыми правами.

Данная сущность предусмотрена для того, чтобы в упрощенной форме представить набор идей, которые дополнительно описываются ниже в подробном описании. Эта сущность не предназначена для того, чтобы идентифицировать ключевые или важнейшие признаки заявляемого предмета изобретения, а также не предназначена для того, чтобы быть использованной в качестве помощи при определении области применения заявляемого предмета изобретения.

### **Краткое описание чертежей**

Фиг. 1 иллюстрирует примерную процедуру регистрации для протокола, с которым изобретаемые варианты осуществления могут быть использованы в одном варианте осуществления.

Фиг. 2 иллюстрирует примерную процедуру обнаружения близости для протокола, с которым изобретаемые варианты осуществления могут быть использованы в одном варианте осуществления.

Фиг. 3 иллюстрирует примерную процедуру установления сеанса для протокола, с которым изобретаемые варианты осуществления могут быть использованы в одном варианте осуществления.

Фиг. 4 иллюстрирует примерную процедуру передачи данных для протокола, с которым изобретаемые варианты осуществления могут быть использованы в одном

варианте осуществления.

Фиг. 5 иллюстрирует аспекты протокола потоковой передачи, с которым изобретаемые варианты осуществления могут быть использованы в соответствии с одним вариантом осуществления.

Фиг. 6 иллюстрирует аспекты, ассоциативно связанные с корневыми лицензиями и листовыми лицензиями в соответствии с одним вариантом осуществления.

Фиг. 7 иллюстрирует аспекты, ассоциативно связанные с корневыми лицензиями и листовыми лицензиями в соответствии с одним вариантом осуществления.

Фиг. 8 иллюстрирует примерный один мультимедийный файл, имеющий семь частей, ассоциативно связанных с пятью различными примерными политиками управления цифровыми правами.

Фиг. 9 иллюстрирует один мультимедийный файл по фиг. 8 с примерными сегментами данных, ассоциативно связанными с ключевыми идентификаторами (KID).

Фиг. 10 иллюстрирует для сегмента данных, показанного на фиг. 9, пакет в соответствии с одним вариантом осуществления.

Фиг. 11 - это блок-схема последовательности операций, показывающая один способ, которым средства предоставляют независимое от содержимого шифрование и расшифровку.

Фиг. 12 иллюстрирует примерное шифрование в соответствии с одним вариантом осуществления.

Фиг. 13 - это блок-схема последовательности операций, иллюстрирующая обмен корневыми и листовыми лицензиями в соответствии с одним вариантом осуществления.

## **Подробное описание изобретения**

### **Обзор**

Описаны средства, которые дают возможность политике управления цифровыми правами быть ассоциативно связанной с цифровым мультимедиа, имеющим произвольный тип содержимого или протокол управления передачей. В некоторых вариантах осуществления средства шифруют сегменты данных мультимедийного файла и добавляют дескриптор в каждый из этих сегментов. Эти дескрипторы могут предоставлять возможность приемному устройству зашифрованного мультимедийного файла расшифровывать файл и потреблять его согласно корректной политике управления цифровыми правами.

В нижеприведенном описании предоставлен раздел, озаглавленный "Протокол защиты содержимого и передачи лицензий", и он описывает одну конкретную систему, в которой могут быть использованы изобретаемые методики. После него предоставлены разделы, озаглавленные "RTSP" и "HTTP", чтобы дать читателю, который не знаком с этими протоколами, понимание изобретаемых методик в этих областях.

После этого раздела предоставлен раздел, озаглавленный "Корневые и листовые лицензии", и он описывает понятие первоначальной корневой лицензии, предоставляющей возможность нескольких других лицензий для мультимедийного файла. После этого раздела предоставлен раздел, озаглавленный "Один зашифрованный мультимедийный файл с несколькими листовыми лицензиями", и он описывает то, как мультимедийный файл может быть ассоциативно связан с более, чем одной политикой управления цифровыми правами с помощью листовых лицензий, ассоциативно связанных с частями мультимедийного файла.

После этих разделов два раздела, первый из которых озаглавлен "Дескрипторы", а

второй озаглавлен "Независимое от содержимого шифрование данных", описывают дескрипторы для сегментов данных мультимедийного файла и способы, которыми средства могут использовать эти дескрипторы, чтобы предоставить шифрование мультимедийного файла независимо от его типа цифрового содержимого. Последний раздел "Использование корневых и листовых лицензий" описывает один способ, которым средства могут использовать корневые и листовые лицензии.

#### **Протокол защиты содержимого и передачи лицензий**

Ниже представлено описание примерного протокола, который предоставляет защиту и передает лицензии для содержимого, протекающего по цифровым линиям связи. Этот протокол составляет только один примерный протокол, с помощью которого могут быть использованы различные изобретаемые методики. Следует принимать во внимание и понимать, что другие протоколы могут быть использованы без отступления от духа и области применения заявляемого предмета изобретения.

Следующие криптографические обозначения используются в данном описании:

$K\{data\}$  - данные зашифрованы с помощью секретного ключа  $K$ .

$K[data]$  - данные подписаны с помощью секретного ключа  $K$ .

$\{data\}_{Device}$  - данные зашифрованы с помощью открытого ключа устройства.

$[data]_{Device}$  - данные подписаны с помощью открытого ключа устройства.

В этом конкретном протоколе предусмотрено пять основных процедур: регистрация, повторная проверка, обнаружение близости, установление сеанса и передача данных.

В процедуре регистрации передающее устройство (т.е. устройство, которое имеет содержимое, которое должно быть передано другому устройству) может уникально и защищенно идентифицировать указанное приемное устройство (т.е. устройство, в которое содержимое должно быть передано). В этом конкретном протоколе передающее устройство хранит базу данных с зарегистрированными приемными устройствами и обеспечивает то, что не более небольшого заранее определенного числа приемных устройств используется одновременно. В ходе процесса регистрации передающее устройство также выполняет процедуру обнаружения близости, чтобы удостовериться в том, что приемное устройство находится "рядом" с передающим устройством в сети, чтобы не допустить широкого распространения защищенного содержимого.

Процедура повторной проверки используется для того, чтобы обеспечить то, что приемное устройство продолжает быть "рядом" с передающим устройством.

Содержимое не доставляется в приемные устройства, если они не зарегистрированы или подвергнуты повторной проверке в течение заранее определенного периода времени в прошлом.

Процедура установления сеанса используется каждый раз, когда приемное устройство запрашивает содержимое от передающего устройства. Передающее устройство осуществляет то, что устройства должны быть зарегистрированы и недавно проверены, до того как установление сеанса может быть завершено.

После того как сеанс установлен, передача данных запрошенного содержимого может выполняться защищенным способом. Приемное устройство может многократно использовать сеанс для того, чтобы извлечь конкретные части содержимого (поиск), но должно установить новый сеанс, чтобы извлечь другое содержимое.

Рассмотрим теперь процедуру регистрации в связи с фиг. 1 и таблицей ниже, которая описывает различные сообщения, которые передаются между передающим

устройством и приемным устройством в ходе регистрации.

| Сообщение                             | Значение      | Описание                                                                                                                      |
|---------------------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------|
| 5<br>Сообщение запроса на регистрацию | Ver           | 8-битовая версия протокола.                                                                                                   |
|                                       | Cert          | Цифровой XML-сертификат приемного устройства.                                                                                 |
|                                       | DId           | 128-битовый серийный номер.                                                                                                   |
| 10<br>Сообщение ответа по регистрации | Ver           | 8-битовая версия протокола.                                                                                                   |
|                                       | {Seed} Device | 128-битовое начальное число, используемое для того, чтобы извлечь ключ шифрования содержимого и ключ целостности содержимого. |
|                                       | SN            | 128-битовый серийный номер.                                                                                                   |
|                                       | Address       | Адрес сокета входящих и исходящих пакетов близости передающего устройства.                                                    |
|                                       | SId           | 128-битовый случайный идентификатор сеанса.                                                                                   |
| 15<br>Алгоритм обнаружения близости   |               | Алгоритм обнаружения близости приводится в исполнение внешним образом.                                                        |

Здесь приемное устройство отправляет сообщение запроса на регистрацию, которое содержит, помимо другой информации, цифровой сертификат приемного устройства. В ответ на прием сообщения запроса на регистрацию передающее устройство проверяет сертификат приемного устройства, формирует начальное число и случайный идентификатор сеанса, возвращая его в форме, указанной выше, в приемное устройство в сообщении ответа по регистрации. После этого приемное устройство проверяет подпись передающего устройства, получает идентификатор сеанса и выполняет другие действия, указанные на чертеже. Приемное устройство и передающее устройство далее могут подвергнуться процессу обнаружения близости, который описан ниже.

В отношении регистрации осуществляются те же процедуры, что и указанные выше, с разницей в том, что в ходе повторной проверки приемное устройство уже зарегистрировано в базе данных.

В отношении обнаружения близости рассмотрим следующее в связи с фиг. 2.

В ходе процедуры обнаружения близости приемное устройство отправляет в передающее устройство сообщение, содержащее идентификатор сеанса, указанный в сообщении инициализации обнаружения близости. Затем передающее устройство отправляет сообщение, содержащее одноразовый номер (128-битовое случайное значение), и измеряет время, которое занимает у приемного устройства ответить одноразовым номером, зашифрованным с помощью ключа шифрования содержимого. В завершение, передающее устройство отправляет сообщение в приемное устройство, указывающее то, успешно или нет обнаружение близости.

Приемное устройство может повторять процесс до тех пор, пока у него не будет подтверждения того, что обнаружение близости выполнено успешно. Когда этот конкретный протокол используется в IP-сетях, сообщения обнаружения близости передаются по UDP. Приемное устройство узнает адрес передающего устройства посредством сообщения ответа по регистрации. Адрес приемного устройства не должен передаваться отдельно, поскольку он может быть определен посредством анализа входящего IP-заголовка UDP-пакета, который переносит сообщение инициализации обнаружения близости.

Таблица ниже описывает сообщения, которые передаются при обнаружении близости:

| Сообщение | Значение | Описание |
|-----------|----------|----------|
|-----------|----------|----------|

|    |                                  |           |                                                                                                             |
|----|----------------------------------|-----------|-------------------------------------------------------------------------------------------------------------|
| 5  | Сообщение начала по близости     | SId       | Такое же 128-битовое значение идентификатора сеанса, что и отправленное посредством передающего устройства. |
|    | Сообщение запроса по близости    | Seq       | 8-битовый инкрементный порядковый номер.                                                                    |
|    |                                  | SId       | Такой же 128-битовый идентификатор сеанса.                                                                  |
|    |                                  | Nonce     | 128-битовое случайное значение.                                                                             |
|    | Сообщение ответа по близости     | Seq       | Такой же порядковый номер, что и определен посредством передающего устройства.                              |
|    |                                  | SId       | Такой же 128-битовый идентификатор сеанса.                                                                  |
|    |                                  | KC{Nonce} | 128-битовый одноразовый номер, зашифрованный с помощью ключа шифрования содержимого.                        |
| 10 | Сообщение результата по близости | SId       | Такой же 128-битовый идентификатор сеанса.                                                                  |
|    |                                  | Result    | Код состояния, указывающий успешность или сбой процедуры регистрации.                                       |

В отношении установления сеанса рассмотрим следующее в связи с фиг. 3 и таблицей ниже, которая описывает сообщения, которые передаются в ходе установления сеанса.

|    |                               |          |                                                                                                                                                                                                        |                                                                                                         |
|----|-------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
|    | Сообщение                     | Значение | Описание                                                                                                                                                                                               |                                                                                                         |
| 20 | Сообщение запроса на лицензию | Ver      | 8-битовая версия протокола.                                                                                                                                                                            |                                                                                                         |
|    |                               | Cert     | Цифровой XML-сертификат приемного устройства.                                                                                                                                                          |                                                                                                         |
|    |                               | SN       | 128-битовый серийный номер.                                                                                                                                                                            |                                                                                                         |
|    |                               | Action   | Запрошенное применение содержимого. Примеры: Play (Воспроизвести), Copy (Копировать) или Burn (Записать).                                                                                              |                                                                                                         |
|    |                               | RId      | 128-битовый случайный идентификатор прав.                                                                                                                                                              |                                                                                                         |
|    |                               | VCRL     | Версия CRL приемного устройства.                                                                                                                                                                       |                                                                                                         |
| 25 | Сообщение ответа по лицензии  | Ver      | 8-битовая версия протокола.                                                                                                                                                                            |                                                                                                         |
|    |                               | CRL      | CRL передающего устройства. Передается только в том случае, если он имеет более высокий номер версии, чем CRL приемного устройства, и компонент приемного устройства также имеет возможности передачи. |                                                                                                         |
|    |                               | License  | KC (зашифрован с помощью открытого ключа приемного устройства).                                                                                                                                        | 128-битовый случайный ключ шифрования содержимого.                                                      |
|    |                               |          | KI (зашифрован с помощью открытого ключа приемного устройства).                                                                                                                                        | 128-битовый случайный ключ целостности содержимого.                                                     |
|    |                               |          | VCRL                                                                                                                                                                                                   | Версия CRL передающего устройства.                                                                      |
|    |                               |          | RId                                                                                                                                                                                                    | Такое же 128-битовое значение идентификатора прав, что и отправленное посредством приемного устройства. |
|    |                               |          | SN                                                                                                                                                                                                     | 128-битовый серийный номер.                                                                             |
| 30 |                               |          |                                                                                                                                                                                                        |                                                                                                         |
| 35 |                               |          |                                                                                                                                                                                                        |                                                                                                         |

В этом примере сообщение запроса на лицензию отправляется от приемного устройства в передающее устройство и содержит информацию, описанную выше. В ответ передающее устройство может отправить сообщение ответа по лицензии, которое содержит информацию, описанную выше.

В этом конкретном примере лицензия представляется в XMR-формате и включает в себя ключ шифрования содержимого, ключ целостности содержимого, версию CRL передающего устройства, 128-битовый идентификатор прав и 128-битовый серийный номер. Лицензия также содержит ОМАС, вычисленный с помощью ключа целостности содержимого с использованием ОМАС.

В отношении процедуры передачи данных рассмотрим следующее в связи с фиг. 4. После того как установление сеанса завершено, передача данных приводится в исполнение конкретным для управляющего протокола способом. И запрос, и ответ по передаче данных должны быть конкретно заданы для управляющего протокола и

типа содержимого. Это концептуально представлено на фиг. 4.

После предоставления краткого обзора примерного протокола, с которым изобретаемые варианты осуществления могут быть использованы, рассмотрим некоторые исходные данные по RTSP.

## RTSP

Протокол потоковой передачи в реальном времени, или RTSP, - это протокол прикладного уровня для управления доставкой непрерывного мультимедиа (к примеру, данных со свойствами реального времени, как потоковая передача), как должны принимать во внимание специалисты в данной области техники. RTSP предоставляет расширяемую инфраструктуру, чтобы предоставить контролируемую доставку данных в реальном времени по запросу, таких как аудио и видео. Источники данных могут включать в себя как "живые" потоки данных, так и сохраненные клипы. Этот протокол предназначен для того, чтобы управлять несколькими сеансами доставки данных, предоставлять средство для выбора каналов доставки, такое как UDP, многоадресный UDP и TCP, и предоставлять средство выбора механизмов доставки на основе RTP.

RTSP устанавливает и контролирует либо однократно, либо несколько раз синхронизированные во времени потоки непрерывного мультимедиа, такие как аудио и видео. Он типично не доставляет сами непрерывные потоки, хотя возможно чередование непрерывного мультимедийного потока с управляющим потоком. Другими словами, RTSP выступает в качестве средства удаленного управления сетью для серверов мультимедиа.

Набор потоков, который должен контролироваться, задается посредством описания представления. В RTSP нет понятия RTSP-соединения; вместо этого сервер поддерживает сеанс, помеченный посредством идентификатора. RTSP-сеанс никоим образом не привязан к соединению транспортного уровня, такому как TCP-соединение. В ходе RTSP-сеанса RTSP-клиент может открывать и закрывать надежные транспортные соединения с сервером, чтобы выдавать RTSP-запросы. Альтернативно, он может использовать транспортный протокол без установления соединения, например, UDP, как должны принимать во внимание специалисты в данной области техники.

Потоки, контролируемые посредством RTSP, могут использовать RTP, но работа RTSP не зависит от механизма транспортировки, используемого для того, чтобы переносить непрерывное мультимедиа.

Рассмотрим теперь типичный обмен запросом/ответом RTSP в связи с фиг. 5 между клиентом/приемным устройством 500 и сервером/передающим устройством 502.

Предварительно запросы/ответы RTSP имеют заголовки, которые не описываются в целях краткости. В RTSP клиент/приемное устройство 500 типично выдает то, что известно как запрос DESCRIBE, который направлен на извлечение описания представления или мультимедийного объекта, идентифицированного посредством URL-адреса запроса от сервера 502. Сервер 502 отвечает описанием запрошенного ресурса, которое представляется в SESSION DESCRIPTION PROTOCOL (SDP). Ответ DESCRIBE (SDP) содержит всю информацию инициализации мультимедиа для ресурса(ов), который он описывает.

Далее клиент 500 отправляет запрос SETUP на URI-адрес, который указывает механизм транспортировки, который должен быть использован для пакетного мультимедиа. В примере по фиг. 5 запрос SETUP отправляется для аудио и видео. Клиент 500 также указывает в запросе SETUP параметры транспортировки, которые

должны быть использованы. Заголовок транспортировки в запросе SETUP указывает параметры транспортировки, допустимые для клиента при передаче данных. RESPONSE от сервера 502 содержит параметры транспортировки, выбранные сервером. Сервер также формирует идентификаторы сеанса в ответ на запросы SETUP.

В этой точке клиент может выдать запрос PLAY, который сообщает серверу начать отправку данных посредством механизма, указанного в SETUP. В ответ на прием запроса PLAY сервер может начать потоковую передачу содержимого, которым является, например, аудио/видеосодержимое. В этом примере потоковое содержимое инкапсулируется с помощью RTP-пакетов и отправляется по UDP, как должны принимать во внимание специалисты в данной области техники.

RTSP-протокол имеет другие представляющие интерес методы, которые включают в себя PAUSE, TEARDOWN, GET\_PARAMETER, SET\_PARAMETER, REDIRECT и RECORD. Для получения дополнительных сведений по RTSP читатель должен обратиться к документу RTSP RFC, Schulzrinne, H., Rao, A. и R. Lanphier, "Real Time Streaming Protocol (RTSP)", RFC 2326, доступному по адресу <http://www.ietf.org/rfc/rfc2326.txt>, апрель 1998 года.

### **Корневые и листовые лицензии**

В проиллюстрированном и описанном варианте осуществления используются понятия корневая лицензия и листовые лицензии. Здесь корневая лицензия используется для того, чтобы устанавливать и защищенно доставлять ключ содержимого (корневой ключ содержимого) клиенту/приемному устройству с тем, чтобы клиент/приемное устройство могло расшифровать впоследствии доставляемую листовую лицензию(и). После того как корневой ключ содержимого защищенно доставлен клиенту/приемному устройству, ключи содержимого для различных листовых лицензий (листовые ключи содержимого) могут быть зашифрованы сервером/передающим устройством с помощью корневого ключа содержимого, отправленного клиенту/приемному устройству. С помощью корневого ключа содержимого клиент может расшифровать листовые ключи содержимого и ассоциативно связанные политики в листовых лицензиях. Каждая из листовых лицензий также имеет уникальный идентификатор, допускающий ассоциативное связывание листовой лицензии с частью мультимедийного файла. Здесь уникальный идентификатор упоминается как ключевой идентификатор, или KID, и предназначен для каждой листовой лицензии, пронумерованной от 1 до n ( $leaf_1, leaf_2, \dots, leaf_n$ ),  $KID_{leaf-n}$ .

Чтобы предоставить один из примеров того, как может быть реализована эта конкретная схема, рассмотрим следующее в связи с фиг. 6. В этом конкретном примере система по фиг. 6 сконфигурирована так, чтобы использовать 1024-битовые RSA-ключи для криптографической операции с открытым ключом и 128-битовые AES-ключи для симметричных криптографических операций. Разумеется, это приведено только в качестве одного примера и не предназначено для того, чтобы ограничивать применение заявляемого предмета изобретения.

В этом примере клиент/приемное устройство 600 имеет пару 650 открытый/закрытый ключ, а сервер/передающее устройство 602 имеет открытый ключ клиента/приемного устройства. В этом примере каждый из открытого и закрытого ключа клиента/приемного устройства является 1024-битовым RSA-ключом. Используя открытый ключ клиента/приемного устройства, сервер/передающее устройство составляет корневую лицензию, которая содержит корневой ключ содержимого, который зашифрован с помощью открытого ключа клиента/приемного устройства.

Корневой ключ содержимого является 128-битовым AES-ключом содержимого. Эта  
корневая лицензия затем отправляется клиенту/приемному устройству. На фиг. 6 это  
показано как первый обмен данными, который осуществляется между  
клиентом/приемным устройством и сервером/передающим устройством, где  
зашифрованный ключ корневого содержимого представляется как  $\{\text{content key}_{\text{root}}\}$   
CLIENT. Тем не менее, следует принимать во внимание, что другой обмен данными до  
проиллюстрированного обмена данными может осуществляться.

После приема и шифрования корневого ключа содержимого от  
сервера/передающего устройства, клиент/приемное устройство теперь может  
расшифровать свой корневой ключ содержимого с помощью открытого ключа и  
может защищенно хранить расшифрованный корневой ключ содержимого для  
будущего использования.

В этой точке рассмотрим, что произошло. Сервер/передающее устройство  
защищенно передал ключ клиенту/приемному устройству, который теперь может  
выступать в качестве основы для последующих криптографических операций. Более  
конкретно, рассмотрим теперь, что несколько конкретных политик могут относиться  
к нескольким конкретным фрагментам DRM-защищенного содержимого в одном  
мультимедийном файле. В этом случае сервер/передающее устройство может  
подготовить несколько листовых лицензий, каждая из которых содержит политику  
управления цифровыми правами и зашифрованную версию конкретного листового  
ключа содержимого. В этом примере каждый листовой ключ содержимого  
является 128-битовым AES-ключом содержимого, который зашифрован с помощью  
корневого ключа содержимого. Таким образом, вычислительная сложность и  
расходы, вызываемые и понесенные клиентом/приемным устройством, ассоциативно  
связанные с расшифровкой новых и дополнительных листовых ключей содержимого,  
снижаются в сравнении с ассоциативно связанными с операциями для 1024-  
битовых RSA-ключей, поскольку теперь клиенту/приемному устройству требуется  
выполнять расшифровку только с помощью 128-битового AES-ключа содержимого  
(т.е. корневого ключа содержимого).

## HTTP

После пояснения понятия корневой и листовой лицензии, а также того, как каждая  
из них может быть использована в контексте, описанном выше, рассмотрим теперь,  
как корневая и листовая лицензия может быть доставлена с помощью HTTP.

Когда HTTP используется для переноса DRM-защищенного содержимого, клиент  
выдает два запроса серверу/передающему устройству. Во-первых, клиент выдает  
запрос POST, чтобы извлечь корневую лицензию. Во-вторых, клиент выдает  
запрос GET для извлечения DRM-защищенного содержимого. Клиент выдает запросы  
в этом примере, поскольку в HTTP сервер типично не может инициировать обмен  
данными с клиентом.

В частности, рассмотрим фиг. 7 в связи с последующим описанием. Когда клиент  
хочет принять корневую лицензию, он выдает запрос POST серверу. Запрос POST  
содержит сообщение запроса на лицензию, как описано выше. В ответ на прием этого  
обмена данными сервер отвечает сообщением ответа по лицензии, которое содержит  
корневую лицензию, которая, по меньшей мере, в одном варианте осуществления  
выражается в XMR. После приема корневой лицензии и ее обработки надлежащим  
образом клиент выдает запрос GET серверу, запрашивая DRM-защищенное  
содержимое. В ответ на запрос GET сервер отвечает сегментами запрошенного  
содержимого, чередующимися с одним или более сообщений ответа по лицензии.

Каждое сообщение ответа по лицензии содержит листовую лицензию, которая относится к конкретной части DRM-защищенного содержимого. Любой подходящий механизм или методика чередования может быть использована для формулирования ответа сервера.

В качестве одного из примеров реализации в одном конкретном контексте рассмотрим следующее.

В одном из примеров четырехбайтовый заголовок кадрирования используется для того, чтобы инкапсулировать данные и управляющие блоки. Заголовок кадрирования содержит однобайтовый ASCII-знак доллара (0x24), после которого следует однобайтовый идентификатор типа блока, за которым следует двухбайтовая длина инкапсулированных данных, представленных в порядке сетевых байтов.

| Секции       | Поля                                      |
|--------------|-------------------------------------------|
| Заголовок    | 8-битовый ASCII-знак доллара (0x24)       |
|              | 8-битовый тип блока                       |
| Длина данных | 16-битовая длина инкапсулированных данных |

Блок управления использует ASCII-символ "с" (0x63) в качестве идентификатора типа. Этот блок содержит сообщение, типично сообщение ответа по лицензии.

Блок данных использует ASCII-символ "d" (0x63) в качестве идентификатора типа. Этот блок содержит дескриптор сегмента данных, сразу за которым следуют мультимедийные данные.

Дескриптор сегмента данных может быть ассоциативно связан с содержимым, которое зашифровано или находится в открытом виде. Зашифрованный флаг в этом дескрипторе переносит эту информацию. Дескриптор сегмента данных ассоциативно связан с частью переданного файла, к которой, если зашифрована, применяется одна политика и ключ шифрования содержимого. Другими словами, ключ шифрования содержимого и политики не могут быть изменены в сегменте.

В соответствии с одним вариантом осуществления, типичный HTTP-ответ с шифрованием линии связи состоит из следующих блоков:

1. Блок управления [\$c], переносящий сообщение ответа по лицензии с цепной лицензией.

2. Один или более блоков данных [\$d].

В случае если произошло изменение ключа или политики в ходе передачи файла, то добавляются следующие этапы:

3. Новый блок управления [\$c], переносящий сообщение ответа по лицензии с новой цепной лицензией.

4. Один или более блоков данных [\$d].

Отметим, что этапы 3 и 4 могут осуществляться несколько раз в случае нескольких изменений ключа или политики.

**Один зашифрованный мультимедийный файл с несколькими листовыми лицензиями**

Средства дают возможность одному зашифрованному мультимедийному файлу иметь части, ассоциативно связанные с различными политиками. Один зашифрованный мультимедийный файл может иметь произвольный тип содержимого (к примеру, ASF, MPEG, WAV или другие файлы) и передаваться с помощью различных протоколов управления.

В проиллюстрированном и описанном ниже варианте осуществления по фиг. 8 один зашифрованный мультимедийный файл 800 имеет семь частей 802, 804, 806, 808, 810, 812 и 814. Допустим, что этот мультимедийный файл является мультимедийной

программой по истории музыкального видео. Первая часть - это введение в музыкальное видео, вторая - это музыкальное видео, третье - это реклама, четвертая - это еще одно музыкальное видео, пятая - это еще одно музыкальное видео, шестая - это еще одна реклама, а седьмая - это заключение к программе.

Здесь автор мультимедийной программы хочет иметь различные права для различных частей. Автор может захотеть разрешить пользователям мультимедийной программы воспроизвести части введения и заключения и скопировать их определенное число раз. Автор может не захотеть предоставить такие же права к музыкальным видео; допустим здесь, что автор программы не владеет этими музыкальными видео, так что они подлежат различным политикам использования. Автор также может захотеть иметь рекламные объявления свободно используемыми, и таким образом они могут быть скопированы, использованы и воспроизведены способом, который требуется пользователю.

Чтобы управлять использованием каждой из этих частей, каждая ассоциативно связывается с политикой. Здесь политика - это листовая лицензия, имеющая KID и ключ содержимого. Допустим, что одна корневая лицензия и пять листовых лицензий принято для этой мультимедийной программы. Листовые лицензии показаны на фиг. 8 как 816, 818, 820, 822 и 824. Каждая из листовых лицензий имеет уникальный KID ( $KID_1$ ,  $KID_2$ ,  $KID_3$ ,  $KID_4$  и  $KID_5$ ) и уникальный листовой ключ содержимого (leaf content key<sub>1</sub>, leaf content key<sub>2</sub>, leaf content key<sub>3</sub>, leaf content key<sub>4</sub> и leaf content key<sub>5</sub>). Каждая листовая лицензия также содержит политику (policy<sub>1</sub>, policy<sub>2</sub>, policy<sub>3</sub>, policy<sub>4</sub> и policy<sub>5</sub>), разрешающую или исключающую конкретные права для использования мультимедиа в каждой из ассоциативно связанных частей. Эти листовые лицензии выражаются в XMR (расширяемые мультимедийные права), хотя также могут быть использованы другие языки.

Первая политика (политика листовой лицензии 1) разрешает воспроизведение мультимедиа, ассоциативно связанного с ней, до десяти раз и копирование до трех раз. Эта политика, следовательно, разрешает введению и заключению программы быть воспроизведенным и скопированным определенное число раз.

Вторая политика разрешает воспроизведение мультимедиа, ассоциативно связанного с ней, только один раз и не разрешает копирование. Таким образом, первое музыкальное видео программы может быть воспроизведено только один раз. Если пользователь попытается воспроизвести всю программу второй раз, это видео не будет воспроизводиться.

Третья политика разрешает воспроизведение мультимедиа, ассоциативно связанного с ней, любым требуемым способом. Сама политика может задать то, что нет ограничений на воспроизведение, копирование или другое использование ассоциативно связанного мультимедиа. Тем не менее, в некоторых вариантах осуществления части мультимедиа вместо этого могут быть открытыми (незашифрованными). Пример этого описан ниже. В любом случае и первое, и второе рекламное объявление могут быть использованы любым требуемым способом.

Четвертая политика разрешает воспроизведение мультимедиа, ассоциативно связанного с ней, столько раз, сколько требуется пользователю, но не разрешает копирование мультимедиа. Таким образом, второе музыкальное видео может быть воспроизведено, но не скопировано.

Пятая политика разрешает воспроизведение мультимедиа, ассоциативно связанного с ней, столько раз, сколько требуется пользователю, и копирование, но только как аналоговый файл. Таким образом, третье музыкальное видео может быть

воспроизведено и скопировано только определенным способом.

Ассоциативная связь между каждой из частей и лицензиями показана на фиг. 8 пунктирной линией. Способы, которыми средства могут устанавливать эту ассоциативную связь, подробнее изложены ниже.

### 5 **Дескрипторы**

Средства могут ассоциативно связывать политики с частями одного мультимедийного файла. Продолжая проиллюстрированный и описанный вариант осуществления по фиг. 8, каждая из частей ассоциативно связывается с политикой посредством листовой лицензии. Чтобы лучше пояснить то, как эта ассоциативная связь может быть установлена, одна часть одного мультимедийного файла 800 проиллюстрирована подробнее.

15 Фиг. 9 иллюстрирует мультимедийный файл 800 с четвертой частью 808 развернутой, чтобы показать один способ, которым эта часть может быть ассоциативно связана с политикой. Здесь мультимедийный файл принимается с частями, в общем, по порядку. В этом примере принимается корневая лицензия, после которой первая листовая лицензия, после которой первая часть мультимедийного файла, после которой вторая листовая лицензия, после которой вторая часть и т.д. 20 Здесь листовые лицензии не все принимаются до приема начала мультимедийного файла, как описано выше. Благодаря этому первая и третья листовые лицензии могут быть отправлены повторно перед частью, ассоциативно связанной с ними (таким образом, первая листовая лицензия может быть отправлена перед первой частью и снова перед седьмой частью).

25 Когда новая политика должна последовать за частью мультимедийного файла, новая листовая лицензия (здесь четвертая листовая лицензия 822) отправляется перед частью мультимедиа, ассоциативно связанной с четвертой листовой лицензией.

Здесь листовая лицензия отправляется как часть блока 902 управления, за которым следуют сегменты 904-914 данных четвертой части 808. Тем не менее, в RTSP лицензии 30 доставляются в дескрипторах SDP или сообщениях ANNOUNCE. Этот конкретный вариант осуществления ориентирован на использование HTTP, хотя использование и обмен корневыми лицензиями и данными также может использовать RTSP, как, например, изложено в описании, относящемся к фиг. 7 выше. Блок управления 35 содержит листовую лицензию 822 по фиг. 8 и 9. Листовая лицензия имеет leaf content key<sub>4</sub>, policy<sub>4</sub> и KID<sub>4</sub>. После приема четвертая листовая лицензия может быть расшифрована с помощью корневого ключа содержимого. KID может отправляться открытым или зашифрованным, но допускающим расшифровку.

40 Каждый из сегментов данных ассоциативно связан с политикой, здесь сегменты 904-914 данных ассоциативно связаны с соответствующей четвертой политикой. Эта ассоциативная связь устанавливается с KID четвертой листовой лицензии. KID или идентификатор, ассоциативно связанный с KID, сохраняется в каждом сегменте данных. KID может быть относительно коротким фрагментом информации, даже 45 целым числом, занимающим меньше байта в запоминающем устройстве. Таким образом, приемное устройство может ассоциативно связывать сегмент данных с соответствующей политикой на основе KID, указывающего соответствующую политику.

50 Дескриптор может быть использован с различными протоколами управления и данных, а также структурами пакетов, существующими на настоящий момент или которые могут быть созданы в будущем. Одним таким примерным протоколом данных является RTP. Здесь дескриптор ориентирован присоединяемым к концу

каждого пакета. В другом варианте осуществления используется протокол управления HTTP. Здесь дескриптор ориентирован присоединяемым к началу каждого кадра.

Фиг. 10 иллюстрирует дескриптор, ассоциативно связывающий сегмент данных с листовой лицензией в соответствии с RTSP.

В этом примере сегмент 1000 данных может включать в себя заголовок 1008 формата рабочих данных RTP и рабочие данные 1010. Здесь рабочие данные и формат рабочих данных зашифрованы, пример чего описан как часть фиг. 11 ниже.

Здесь дескриптор присоединяется к концу рабочих данных согласно RTP-протоколу, хотя он может быть помещен в любой надлежащей позиции, разрешенной протоколом данных. Помещение дескриптора в конец рабочих данных может смягчать проблемы обратной совместимости, как должны принимать во внимание специалисты в данной области техники.

В этом варианте осуществления RTP-пакет (за исключением RTP-заголовка) ассоциативно связан с дескриптором 1012. Дескриптор 1012, в свою очередь, переносит с собой параметры шифрования, которые могут быть использованы в процессе расшифровки, который позволяет рабочим данным 1010 и заголовку 1008 формата рабочих данных RTP быть расшифрованным (к примеру, вектор инициализации (IV), ассоциативно связанный с четвертым листовым ключом содержимого). В этом конкретном примере одна политика и ключ шифрования содержимого применяется к рабочим данным 1010.

В соответствии с одним вариантом осуществления дескриптор 1012 содержит следующую структуру данных:

| Секции     | Поля                                  |
|------------|---------------------------------------|
| Флаги      | 8-битовые флаги                       |
| Расширения | 8-битовое число расширений            |
|            | Несколько расширений переменной длины |
| Длина      | Длина дескриптора сегмента данных     |

В этом примере раздел "Флаги" - это битовое поле, указывающее атрибуты сегмента данных. Следующий бит в настоящее время задан: бит 0 (зашифрованные данные). Когда этот бит задается равным 1, это указывает, что сегмент данных находится в зашифрованной форме. В противном случае сегмент данных является открытым.

Секция расширений содержит KID и IV; здесь KID - это KID<sub>4</sub>, а IV ассоциативно связан с leaf content key<sub>4</sub>.

В отношении секции "Расширения" поле "число расширений" указывает число расширений переменной длины, включенных в этот дескриптор. В отношении поля "Расширение переменной длины", каждое расширение имеет следующий формат:

| Поля                        |
|-----------------------------|
| 8-битовый тип расширения    |
| 16-битовая длина расширения |
| Расширение переменной длины |

В соответствии с одним вариантом осуществления KID и IV задаются следующим образом:

**KID**

Extension Type (Тип расширения). Должен быть равным 1 для расширения

идентификатора ключа.

Extension Length (Длина расширения). Должна быть равна 16, что представляет 128 битов (16 байтов).

Extension (Расширение). Должно содержать значение идентификатора ключа для зашифрованного мультимедиа, доставленного вместе с дескриптором. Это расширение используется только тогда, когда флаг зашифрованных данных равен 1.

#### **Вектор инициализации (IV)**

Extension Type (Тип расширения). Должен быть равным 2 для расширения вектора инициализации.

Extension Length (Длина расширения). Должна быть равна 8, что представляет 64 бита (8 байтов).

Extension (Расширение). Должно содержать вектор инициализации для зашифрованного мультимедиа, доставленного вместе с дескриптором. Это расширение используется только тогда, когда флаг зашифрованных данных равен 1.

В отношении секции "Длина", в этом варианте осуществления данная секция должна содержать общую длину дескриптора в байтах. Эта длина не включает в себя размер мультимедийных данных, доставляемых в связи с данным дескриптором.

#### **Независимое от содержимого шифрование данных**

Фиг. 11 - это блок-схема последовательности операций, которая описывает этапы способа в соответствии с одним вариантом осуществления. Данный способ может быть осуществлен в связи с любыми надлежащими аппаратными средствами, программным обеспечением, микропрограммным обеспечением или их комбинацией. В одном варианте осуществления способ может быть реализован в связи с системами, такими как проиллюстрированные и описанные выше. Дополнительно, в нижеприведенном описании некоторые действия, которые выполняются, проиллюстрированы как выполняемые сервером/передающим устройством, а другие проиллюстрированы как выполняемые клиентом/приемным устройством. Примеры серверов/передающих устройств и клиентов/приемных устройств предоставлены выше.

Этап 1102 принимает мультимедийный файл. Мультимедийный файл может иметь любой тип содержимого, разрешающий разбиение мультимедийного файла на сегменты данных, шифрование, передачу, получение и расшифровку. Это может быть, например, файл ASF, MPEG2 TS, MPEG2 ES или WAV.

Этап 1104 разделяет мультимедийный файл на сегменты данных. Эти сегменты данных могут содержать пакеты, другие фрагменты данных или кадры, соответствующие различным протоколам управления, таким как RTP или HTTP.

Этап 1106 шифрует каждый сегмент данных. Этап 1106 может выполнять это согласно любому из вариантов осуществления, описанных в данном документе. Таким образом, он может шифровать рабочие данные с помощью листового ключа содержимого и шифровать этот листовой ключ содержимого с помощью корневого ключа содержимого. При помощи корневого ключа содержимого приемное устройство может впоследствии расшифровать листовой ключ содержимого и использовать этот листовой ключ содержимого для того, чтобы расшифровать рабочие данные.

В одном варианте осуществления этап 1106 зашифровывает каждый сегмент данных или его часть с помощью AES в режиме подсчета. Фиг. 12 иллюстрирует процесс шифрования одного сегмента данных с помощью этой методики. В этом варианте осуществления режим подсчета создает поток байтов, которые затем подвергаются операции XOR с помощью байтов открытого текста сегмента данных,

чтобы создать зашифрованный сегмент данных. Генератор потока ключей использует округление AES, чтобы сформировать 16-байтовые блоки потока ключей за раз. Входные данные в округление AES - это ключ шифрования содержимого ( $K_C$ ) (к примеру, листовой ключ содержимого) и 128-битовая конкатенация идентификатора сегмента данных ID и номера блока в сегменте данных.

Выходные данные генератора потока ключей должны быть подвергнуты операции XOR побайтово с помощью данных из соответствующего блока сегмента данных. В случае, если сегмент данных не делится равномерно по 16 байтов, только допустимые байты мультимедийных данных из последнего блока должны быть подвергнуты операции XOR с помощью потока ключей и сохранены для зашифрованного сегмента данных.

Этап 1108 добавляет дескриптор в каждый зашифрованный сегмент данных. Дескриптор может содержать KID, IV или другие элементы, изложенные в данном документе. Каждый дескриптор указывает ассоциативно связанную политику управления цифровыми правами, посредством которой должны администрироваться рабочие данные сегмента данных. Эта политика управления цифровыми правами, согласно одному вышеприведенному варианту осуществления, содержится в ранее принятой листовой лицензии. Каждый дескриптор также может указывать ключ содержимого (к примеру, конкретный листовой ключ содержимого), используемый для того, чтобы расшифровать сегмент данных.

Отметим, что результатом этих этапов может быть мультимедийный файл произвольного типа содержимого, разбитый на сегменты данных, причем каждый сегмент данных зашифрован и имеет дескриптор, посредством которого зашифрованные данные в дальнейшем могут быть ассоциативно связаны с политикой управления цифровыми правами.

В одном варианте осуществления дескриптор содержит индикатор длины. С помощью этого индикатора длины приемное устройство зашифрованного сегмента данных может определить, когда дескриптор заканчивается или начинается. Данный индикатор длины дает возможность добавления дескриптора в зашифрованный сегмент данных в различных позициях сегмента данных или его пакета. Для RTP-протокола, например, дескриптор добавляется в конец RTP-пакета, имеющего сегмент данных. Для HTTP-протокола, например, дескриптор добавляется в начало кадра, имеющего сегмент данных. Отметим, что дескриптор за счет наличия различной длины может быть добавлен в различные части сегмента данных и тем самым предоставляет использование дескриптора с различными протоколами передачи.

Этап 1110 передает зашифрованные сегменты данных (и открытые сегменты данных, если есть) с дескрипторами в приемное устройство. Приемное устройство может ориентировать (к примеру, размещать в корректном порядке) сегменты данных способами, известными в данной области техники. Приемное устройство может расшифровывать сегменты данных с помощью ключа содержимого, ассоциативно связанного с сегментами данных.

Дополнительно, приемное устройство с помощью этого дескриптора может определять то, какая политика прав должна быть использована с мультимедийным файлом или его частью. Если мультимедийный файл имеет части, которые должны управляться посредством различных политик прав, этот способ также может разделить сегменты данных на основе их части мультимедийного файла и назначить различные дескрипторы сегментам данных различных частей на этапе 1104.

Этап 1112 принимает и расшифровывает зашифрованные сегменты данных.

Приемное устройство (такое как клиент/приемное устройство 500 или 600) расшифровывает сегменты данных и назначает соответствующую политику прав им на основе их дескриптора. В одном варианте осуществления приемное устройство расшифровывает сегменты данных с помощью вектора инициализации в дескрипторе.

5 Приемное устройство определяет соответствующий листовой ключ содержимого на основе KID, который он далее использует для того, чтобы расшифровывать сегменты данных после расшифровки листового ключа содержимого с помощью корневого ключа содержимого.

10 Этап 1114 ассоциативно связывает каждый сегмент данных с политикой прав. В одном варианте осуществления приемное устройство осуществляет это с помощью идентификатора ключа (KID), обнаруженного в дескрипторе и в листовой лицензии, имеющей политику прав.

#### **Использование корневых и листовых лицензий**

15 Фиг. 13 - это блок-схема последовательности операций, которая описывает этапы способа в соответствии с одним вариантом осуществления. Данный способ может быть осуществлен в связи с любыми надлежащими аппаратными средствами, программным обеспечением, микропрограммным обеспечением или их комбинацией.

20 В одном варианте осуществления способ может быть реализован в связи с системами, такими как проиллюстрированные и описанные выше. Дополнительно, в нижеприведенном описании некоторые действия, которые выполняются, проиллюстрированы как выполняемые сервером/передающим устройством, а другие проиллюстрированы как выполняемые клиентом/приемным устройством. Примеры серверов/передающих устройств и клиентов/приемных устройств предоставлены выше.

25 Этап 1300 расшифровывает корневой ключ содержимого с помощью открытого ключа клиента/приемного устройства. Любой подходящий ключ содержимого может быть использован с одним из примеров, предоставленных выше. Этап 1302 отправляет корневую лицензию, содержащую зашифрованный корневой ключ содержимого,

30 клиенту/приемному устройству. Любой надлежащий способ может быть использован для того, чтобы реализовать этот этап. В нижеприведенном пояснении предоставлены два примера, которые заимствуют два различных протокола. Следует принимать во внимание, что они составляют примеры и не предназначены для того, чтобы

35 ограничивать применение заявляемого предмета изобретения только конкретными протоколами, которые описаны.

Этап 1304 принимает корневую лицензию, отправленную сервером/передающим устройством, а этап 1306 расшифровывает зашифрованный корневой ключ

40 содержимого. В этом примере данный этап осуществляется посредством использования закрытого ключа клиента/приемного устройства для того, чтобы расшифровать зашифрованный корневой ключ содержимого.

Этап 1308 подготавливает листовую лицензию и зашифровывает листовой ключ содержимого с помощью корневого ключа содержимого. Этап 1310 отправляет

45 листовую лицензию клиенту/приемному устройству. Напомним, что листовая лицензия может и типично содержит политики для DRM-защищенного содержимого. Следует понимать и принимать во внимание то, что этапы 1308 и 1310 могут быть приведены в исполнение несколько раз для данного фрагмента DRM-защищенного содержимого.

50 Т.е. для каждой части, имеющей различную политику, соответствующая листовая лицензия может быть подготовлена и отправлена клиенту/приемному устройству.

Этап 1312 принимает листовую лицензию, а этап 1314 расшифровывает листовой ключ содержимого, который ранее принят. Этап 1316 затем использует

расшифрованный листовой ключ содержимого для того, чтобы расшифровать содержимое. Он также ассоциативно связывает соответствующую листовую лицензию с частью мультимедийного файла (если мультимедийный файл имеет части) с помощью дескриптора, описанного выше.

Следует принимать во внимание и понимать, что этапы 1312, 1314 и 1316 могут быть выполнены для каждой новой листовой лицензии, которая принимается клиентом/приемным устройством.

### **Заключение**

Данный документ описывает методики, посредством которых политика управления цифровыми правами может быть ассоциативно связана с цифровым мультимедиа, имеющим произвольный тип содержимого или протокол управления передачей. В некоторых случаях это позволяет приемному устройству зашифрованного мультимедийного файла расшифровывать файл и потреблять части файла согласно различным политикам управления цифровыми правами. В некоторых случаях это также позволяет передающему устройству зашифровывать множество различных типов мультимедийных файлов с помощью одного набора методик. Хотя изобретение было описано на языке, характерном для структурных признаков и/или методологических действий, необходимо понимать, что изобретение, определенное в прилагаемой формуле изобретения, необязательно ограничено описанными характерными признаками или этапами. Наоборот, характерные признаки и этапы раскрываются как предпочтительные формы реализации заявленного изобретения.

### **Формула изобретения**

1. Машинореализованный способ связывания политики управления цифровыми правами с цифровым мультимедиа с использованием компьютера клиента-приемника, имеющего пару открытый/закрытый ключ, и, по меньшей мере, одного компьютера сервера-передатчика, имеющего открытый ключ компьютера клиента-приемника, содержащий этапы, на которых:

формируют корневой ключ содержимого с использованием открытого ключа компьютера клиента-приемника,

передают корневой ключ содержимого на компьютер клиент-приемник, причем корневой ключ содержимого расшифровывается с использованием закрытого ключа компьютера клиента-приемника и используется компьютером клиентом-приемником для расшифровывания листового ключа содержимого;

- зашифровывают сегменты данных мультимедийного файла, чтобы предоставить зашифрованные сегменты данных, причем каждый сегмент данных зашифрован посредством соответствующего листового ключа содержимого; и

- добавляют дескрипторы к каждому из зашифрованных сегментов данных, причем каждый из дескрипторов зашифрованных сегментов данных идентифицирует листовой ключ содержимого, посредством которого сегмент данных был зашифрован, и связанную политику управления цифровыми правами.

2. Способ по п.1, в котором шифрование сегментов данных использует AES в режиме подсчета.

3. Способ по п.1, в котором каждый из дескрипторов содержит векторы инициализации, при этом каждый вектор инициализации связан с идентификатором ключа, идентифицирующим соответствующую назначенную политику управления правами.

4. Способ по п.1, в котором каждый из дескрипторов имеет идентификатор ключа,

который также имеет связанную политику управления цифровыми правами.

5. Способ по п.1, в котором каждый из дескрипторов содержит индикатор длины, обеспечивающий дифференцирование между зашифрованным сегментом данных и каждым из дескрипторов.

6. Способ по п.1, в котором зашифрованные сегменты данных содержат, по меньшей мере, один пакет, соответствующий RTF-протоколу данных, или кадр, соответствующий HTTP-протоколу.

7. Способ по п.6, в котором этап добавления дескрипторов конкатенирует каждый из дескрипторов к концу зашифрованных сегментов данных, если зашифрованные сегменты данных содержат пакет, соответствующий RTF-протоколу, или к началу зашифрованных сегментов данных, если зашифрованные сегменты данных содержат кадр, соответствующий HTTP-протоколу.

8. Система связывания политики управления цифровыми правами с цифровым мультимедиа, содержащая один или более машиночитаемых носителей, при этом машиночитаемые носители содержат цифровой мультимедийный файл, содержащий один или более сегментов данных, причем каждый из сегментов данных добавляется к дескриптору и содержит

рабочие данные, зашифрованные посредством листового ключа содержимого, причем каждый листовой ключ содержимого зашифрован с помощью корневого ключа содержимого, который зашифрован с использованием открытого ключа и расшифровывается с использованием закрытого ключа из пары открытый/закрытый ключ, при этом каждый дескриптор включает в себя, по меньшей мере, связанный листовой ключ содержимого, обеспечивающий возможность расшифровки зашифрованных рабочих данных и связывания зашифрованных рабочих данных с политикой управления цифровыми правами.

9. Система по п.8, в которой каждый дескриптор содержит идентификатор ключа, который идентифицирует политику управления цифровыми правами.

10. Система по п.8, в которой каждые рабочие данные зашифрованы с использованием ключа содержимого и каждый дескриптор содержит идентификатор ключа, связанный с листовым ключом содержимого, который используется для того, чтобы расшифровать зашифрованные рабочие данные.

11. Система по п.8, в которой цифровой мультимедийный файл дополнительно содержит одну или более частей, причем каждая из первых частей имеет один или более сегментов данных и причем дополнительно каждый дескриптор обеспечивает возможность каждой из частей быть связанной с политикой управления цифровыми правами.

12. Система по п.8, в которой каждый из сегментов данных рабочих данных зашифрован, а их дескриптор не зашифрован.

13. Система по п.8, в которой цифровой мультимедийный файл дополнительно содержит один или более сегментов данных, добавленных к дескриптору, и содержит открытые рабочие данные, при этом дополнительно каждый дескриптор сегмента данных обеспечивает возможность связывания открытых рабочих данных с политикой управления цифровыми правами.

14. Система по п.8, в которой цифровой мультимедийный файл - это потоковое мультимедиа.

15. Машинореализованный способ для защищенной передачи мультимедийного файла с множеством частей компьютеру клиенту-приемнику от компьютера сервера-передатчика, содержащий этапы, на которых:

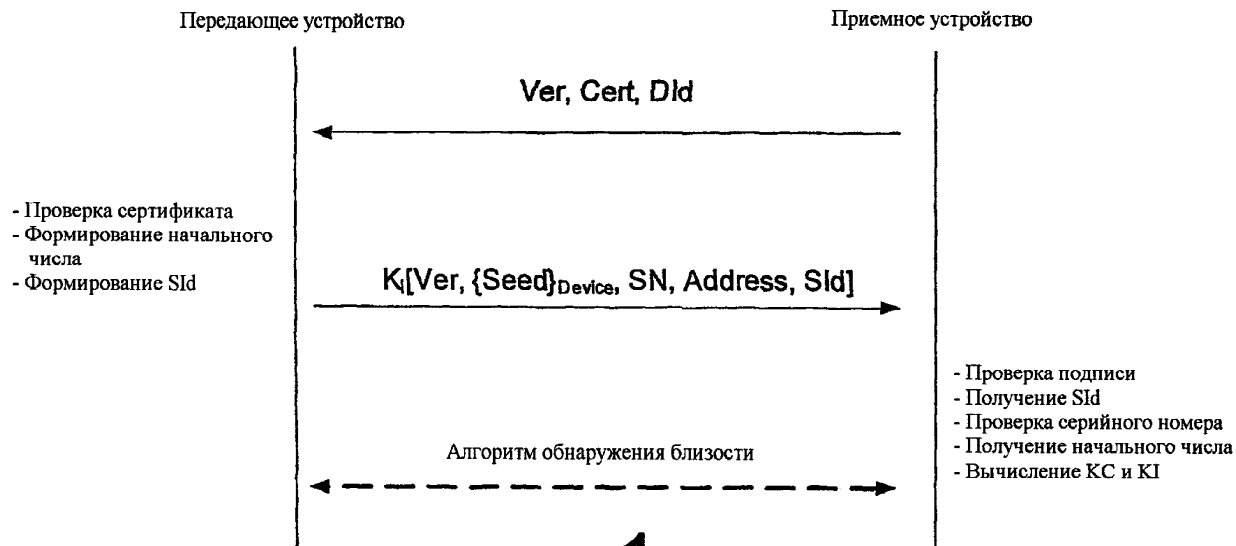
шифруют корневой ключ содержимого с использованием открытого ключа компьютера клиента-приемника, причем корневой ключ содержимого расшифровывается с использованием закрытого ключа компьютера клиента-приемника;

5 передают корневой ключ содержимого компьютера клиента-приемника;  
формируют множество листовых ключей содержимого, причем каждый листовой ключ содержимого формируется для связанной части мультимедийного файла, причем формирование каждого листового ключа содержимого содержит шифрование  
10 каждого листового ключа содержимого посредством корневого ключа содержимого;  
формируют дескриптор для каждой части мультимедийного файла, причем каждый дескриптор идентифицирует листовой ключ содержимого и назначенную политику управления правами, указывающую разрешенное использование связанной части;  
шифруют каждую часть мультимедийного файла посредством связанного  
15 листового ключа содержимого;  
передают зашифрованные части и дескрипторы компьютеру клиенту-приемнику и расшифровывают с помощью компьютера клиента-приемника каждый листовой ключ содержимого с использованием корневого ключа содержимого и  
20 расшифровывают каждую из частей с использованием связанного ключа листового ключа содержимого, уточненного в дескрипторе, связанном с каждой частью.

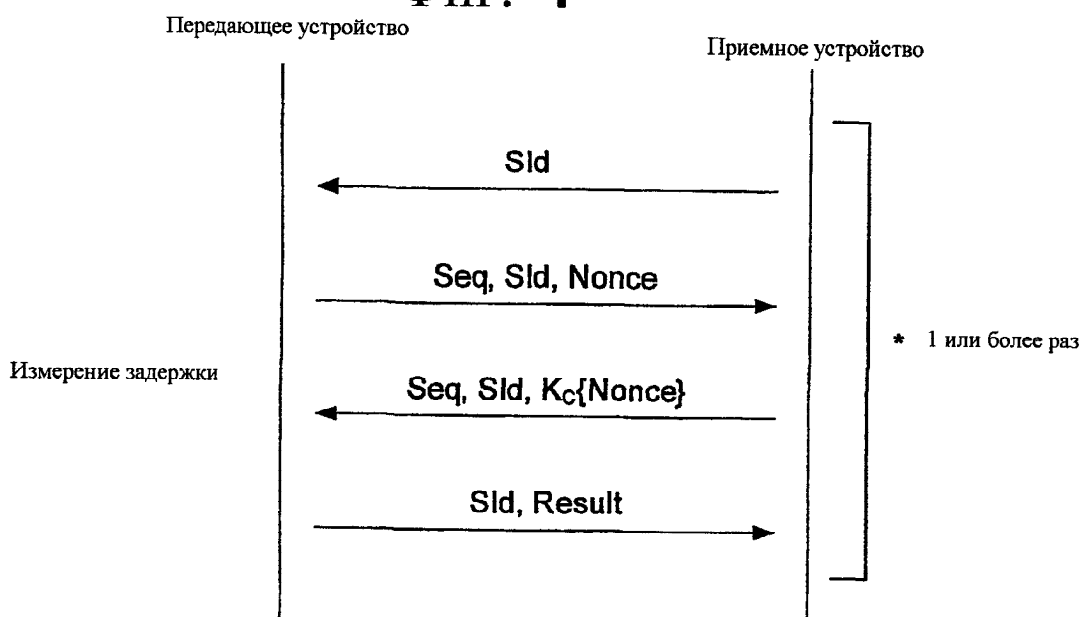
16. Способ по п.15, дополнительно содержащий этап, на котором передают назначенную политику прав в компьютер клиент-приемник.

25 17. Способ по п.15, в котором расшифровка каждой из частей встраивает идентификатор ключа в дескриптор для каждой из частей, причем идентификатор ключа используется компьютером клиентом-приемником для связывания части с соответствующей назначенной политикой прав.

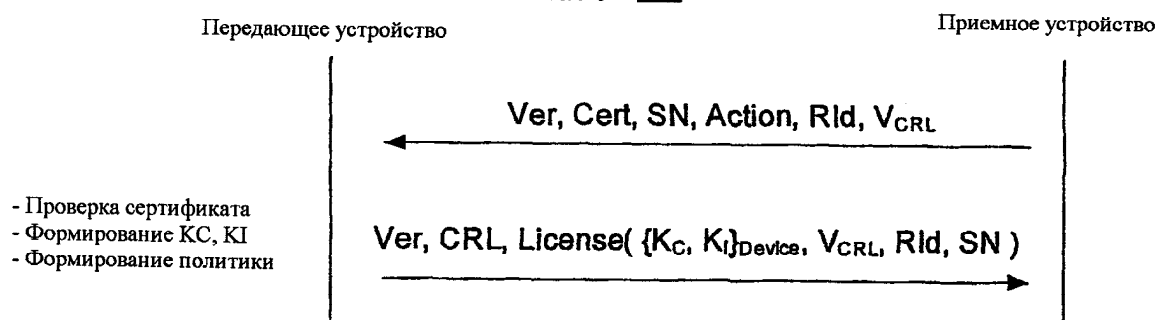
18. Способ по п.15, дополнительно содержащий этап, на котором принимают  
30 мультимедийный файл произвольного типа содержимого и зашифровывают мультимедийный файл, чтобы предоставить зашифрованный мультимедийный файл.



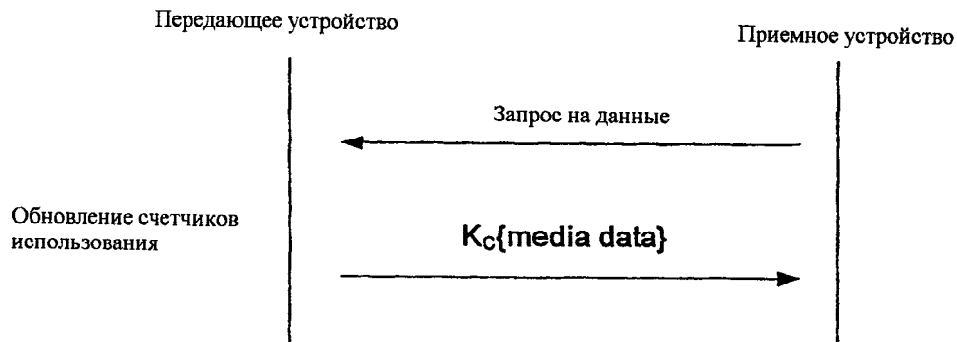
ФИГ. 1



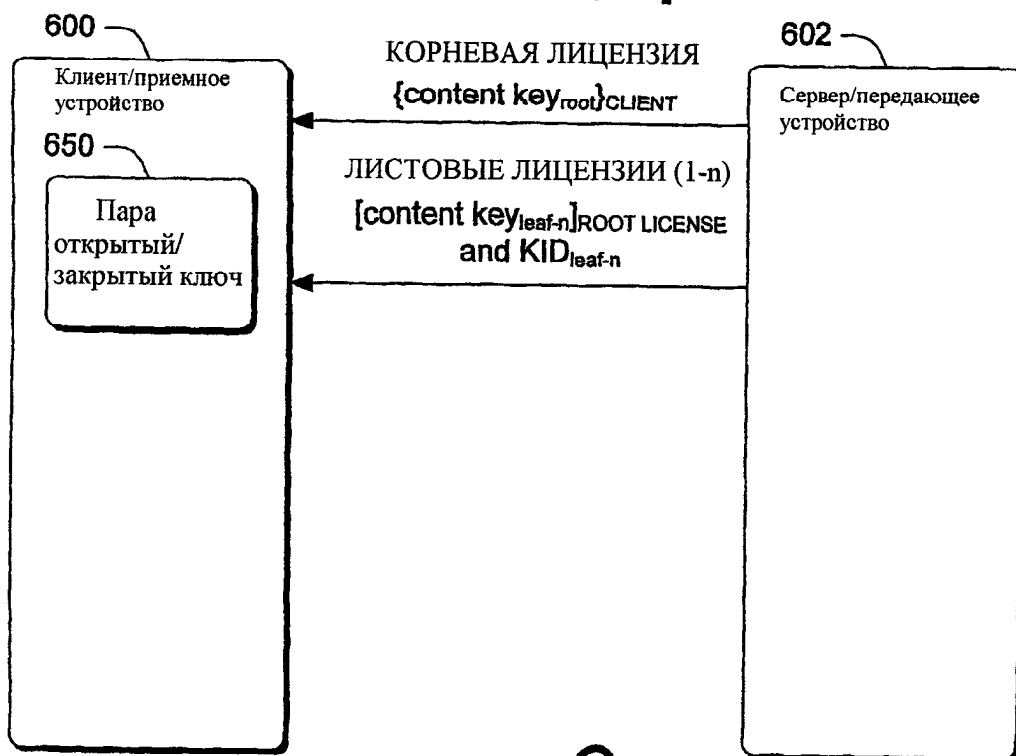
ФИГ. 2



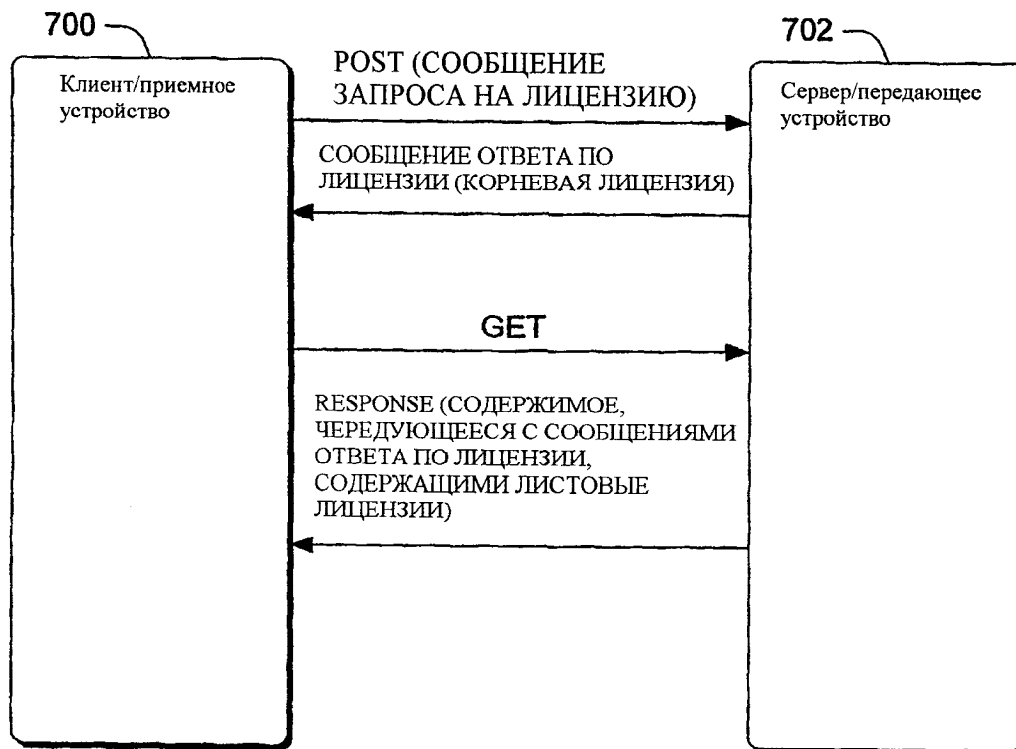
ФИГ. 3



ФИГ. 4



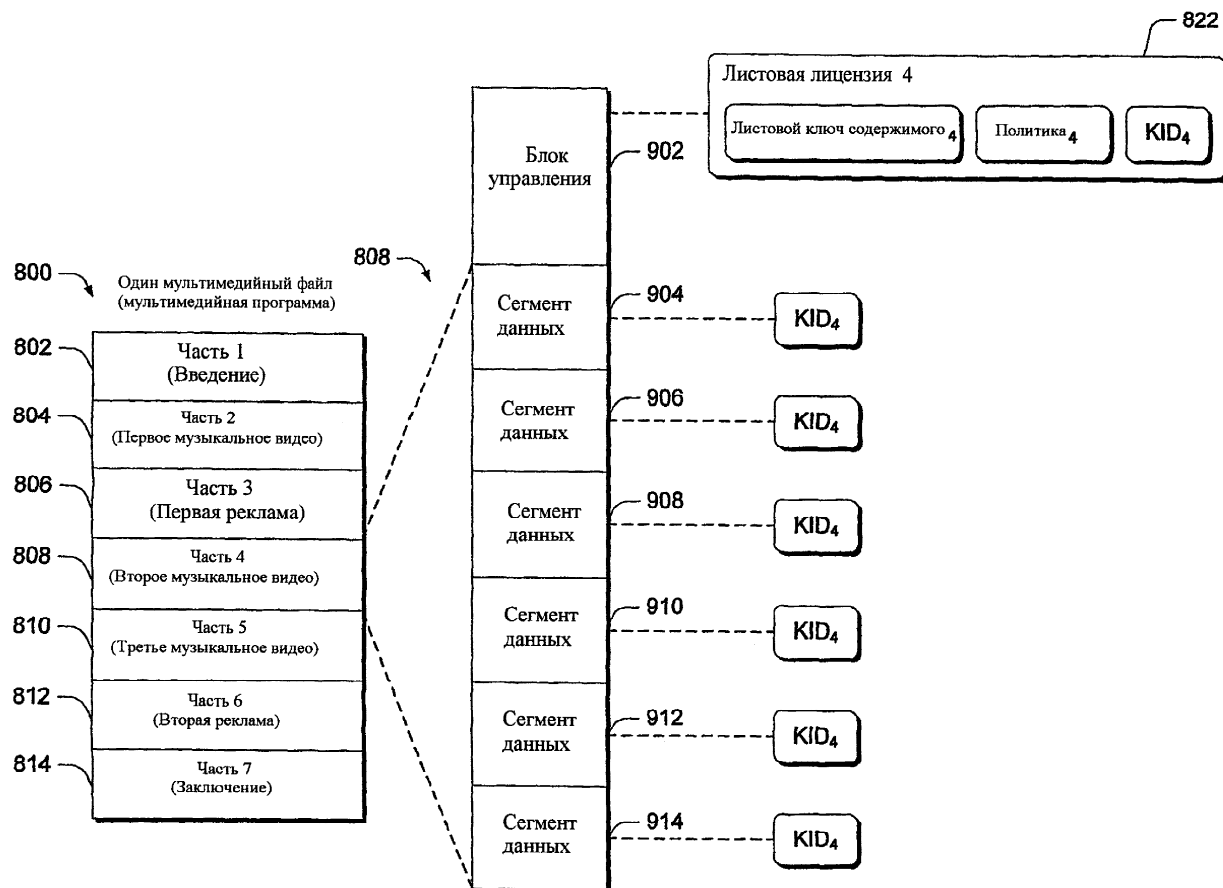
ФИГ. 6



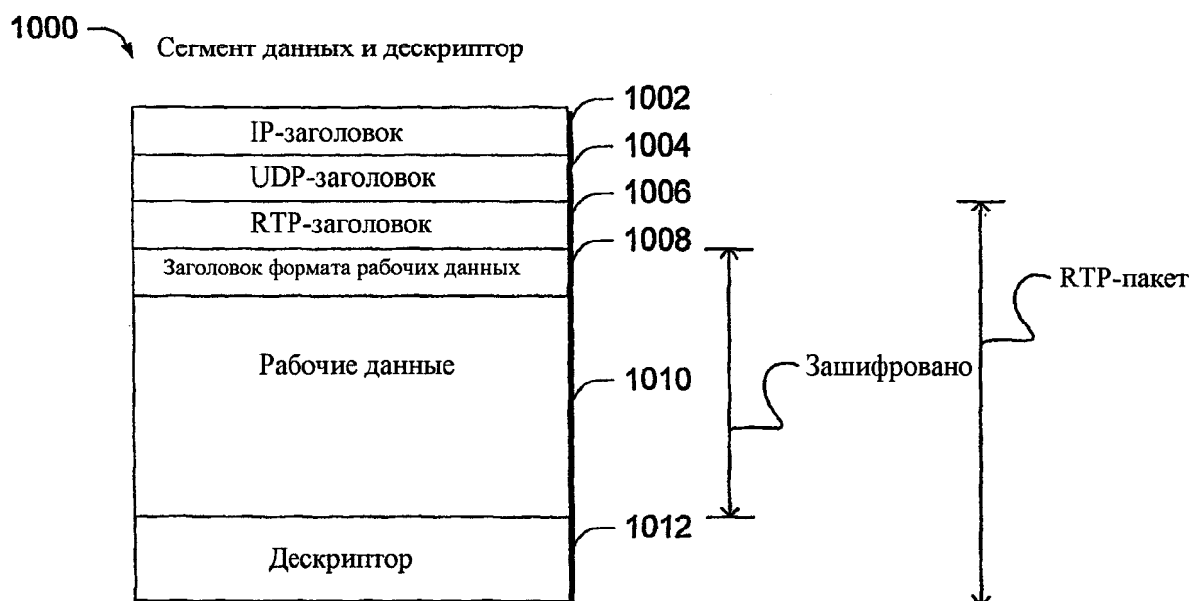
Фиг. 7



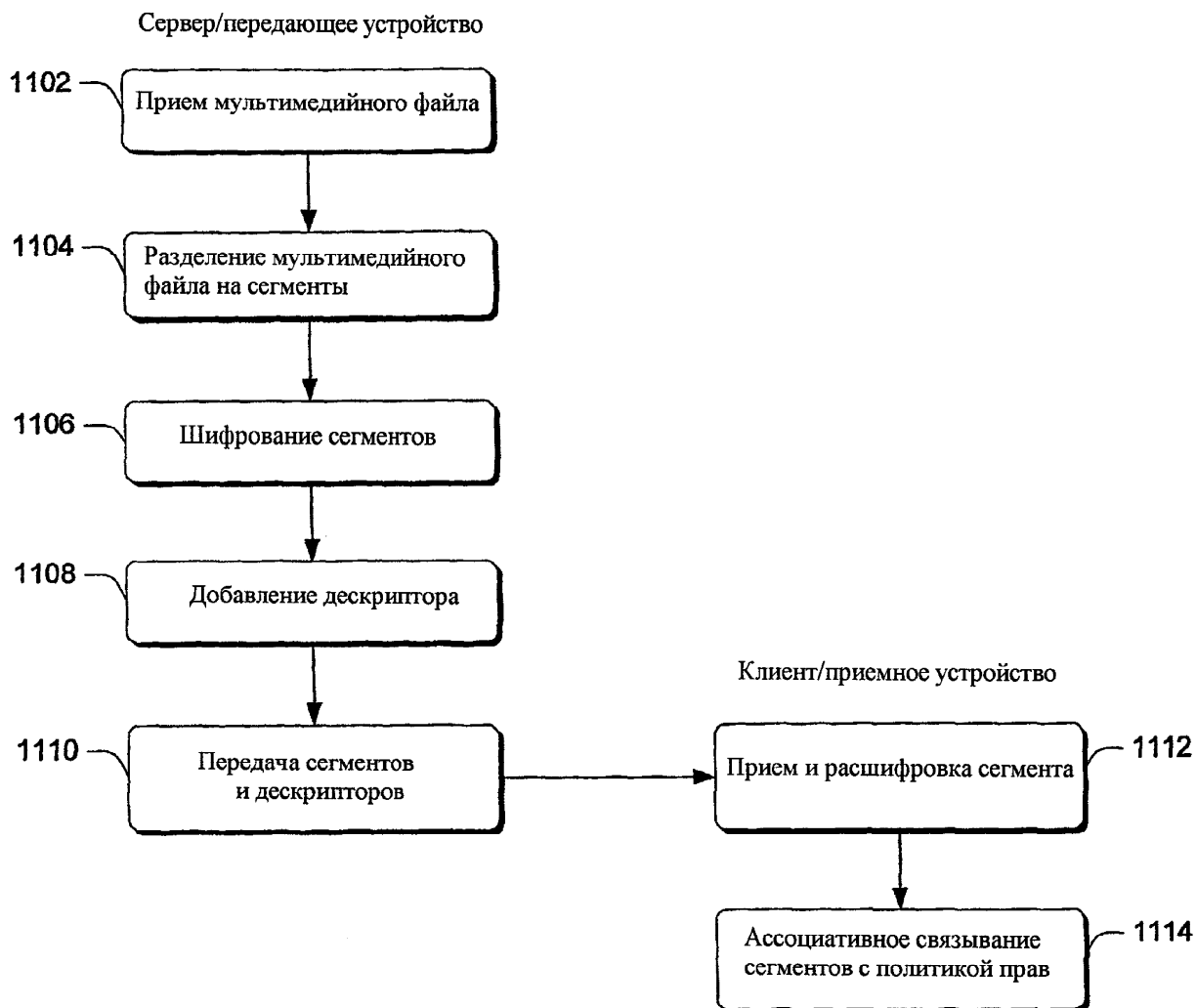
Фиг. 8



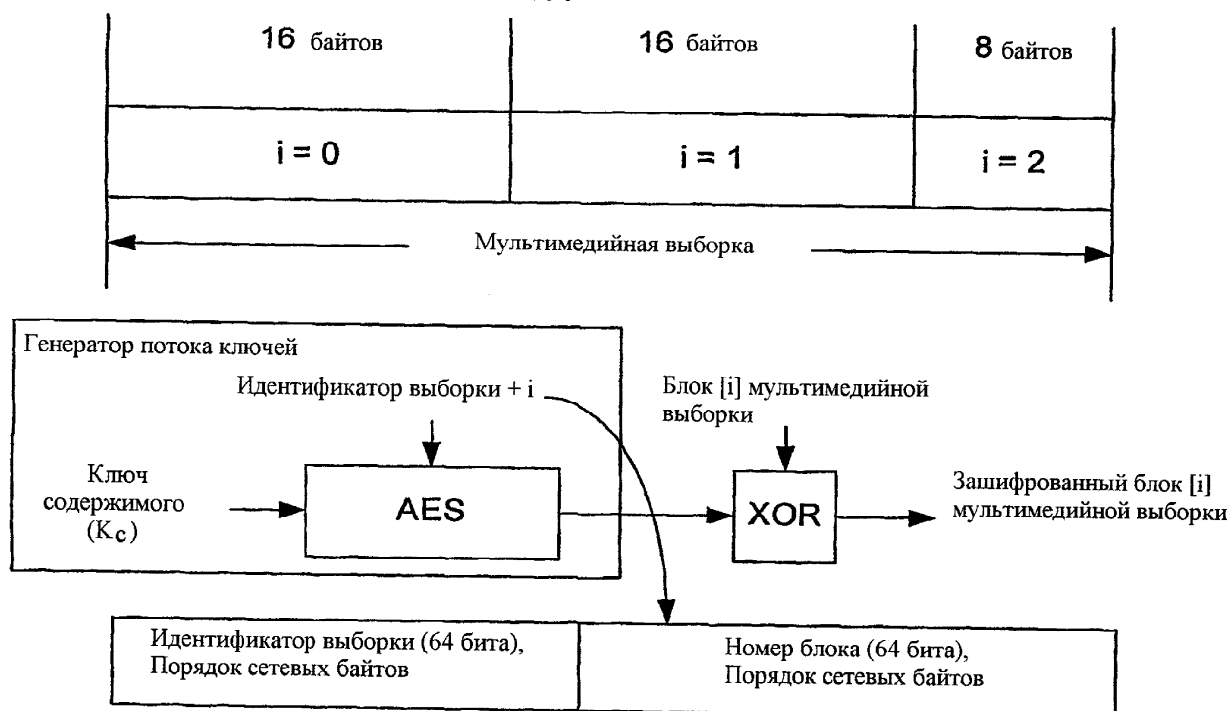
Фиг. 9



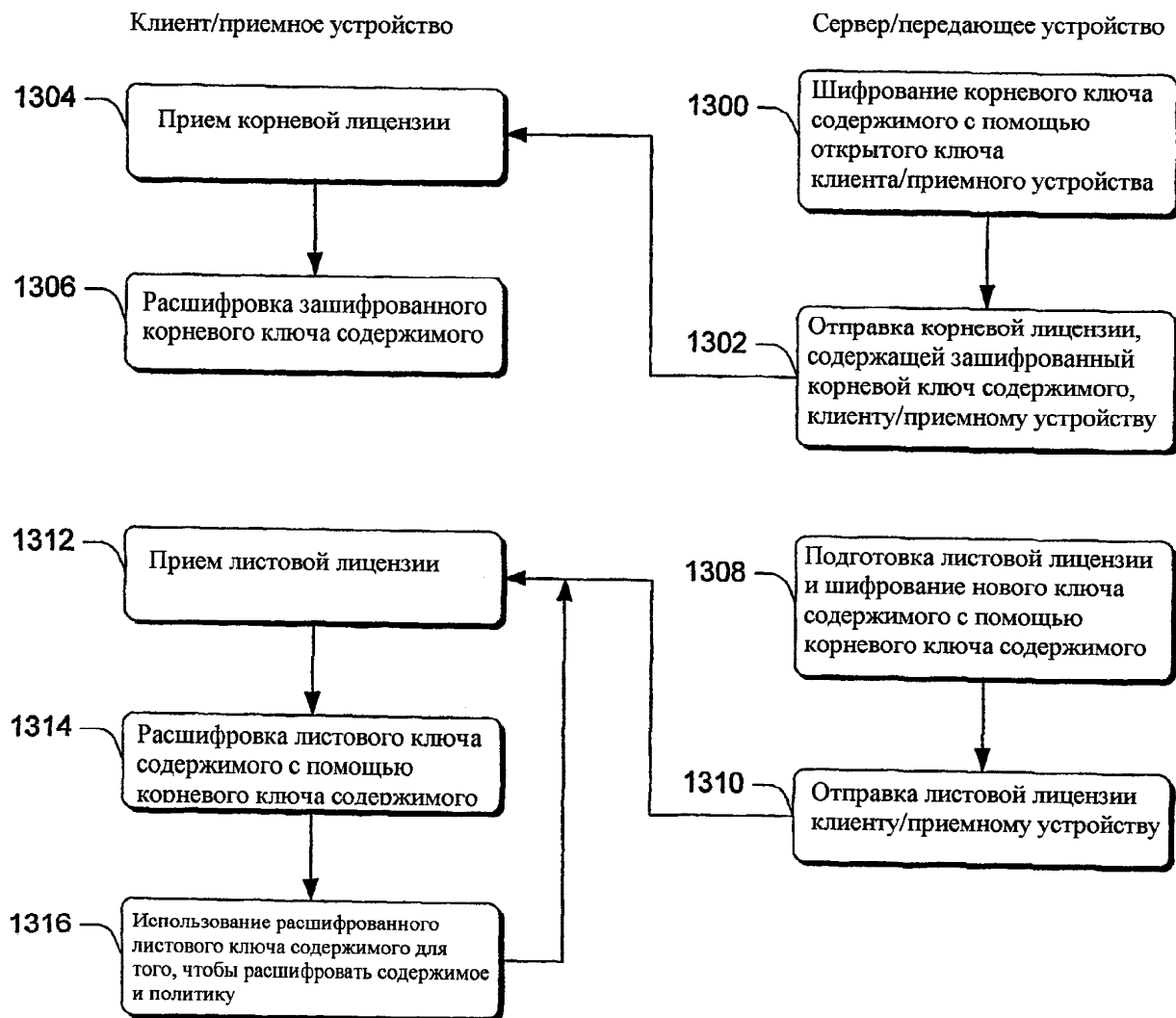
Фиг. 10



ФИГ. 11



ФИГ. 12



Фиг. 13