РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 447 498** (13) **C2**

(51) МПК
G06F 21/00 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2008147396/08, 25.04.2007**

(24) Дата начала отсчета срока действия патента:
25.04.2007

Приоритет(ы):
(30) Конвенционный приоритет:
02.05.2006 EP 06113373.2

(43) Дата публикации заявки: **10.06.2010** Бюл. № 16

(45) Опубликовано: **10.04.2012** Бюл. № 10

(56) Список документов, цитированных в отчете о поиске: **WO 03098931 A1, 27.11.2003. WO 2005088896 A1, 22.09.2005. WO 03077470 A1, 18.09.2003. RU 2260918 C2, 20.09.2005.**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **02.12.2008**

(86) Заявка PCT:
IB 2007/051533 (25.04.2007)

(87) Публикация заявки PCT:
WO 2007/125486 (08.11.2007)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. А.В.Мицу, рег. №364

(72) Автор(ы):
КОСТЕР Роберт П. (NL),
МОНТАНЕР Хавьер (NL),
ЯКОБ Сорин М. (NL),
КОРАЙХИ Найиб (NL)

(73) Патентообладатель(и):
КОНИНКЛЕЙКЕ ФИЛИПС ЭЛЕКТРОНИКС Н.В. (NL),
ВОДАФОН ЛИБЕРТЕЛ Б.В. (NL),
СТИХТИНГ ТЕЛЕМАТИКА ИНСТИТЬЮТ (NL)

(54) УЛУЧШЕННЫЙ ДОСТУП К ДОМЕНУ

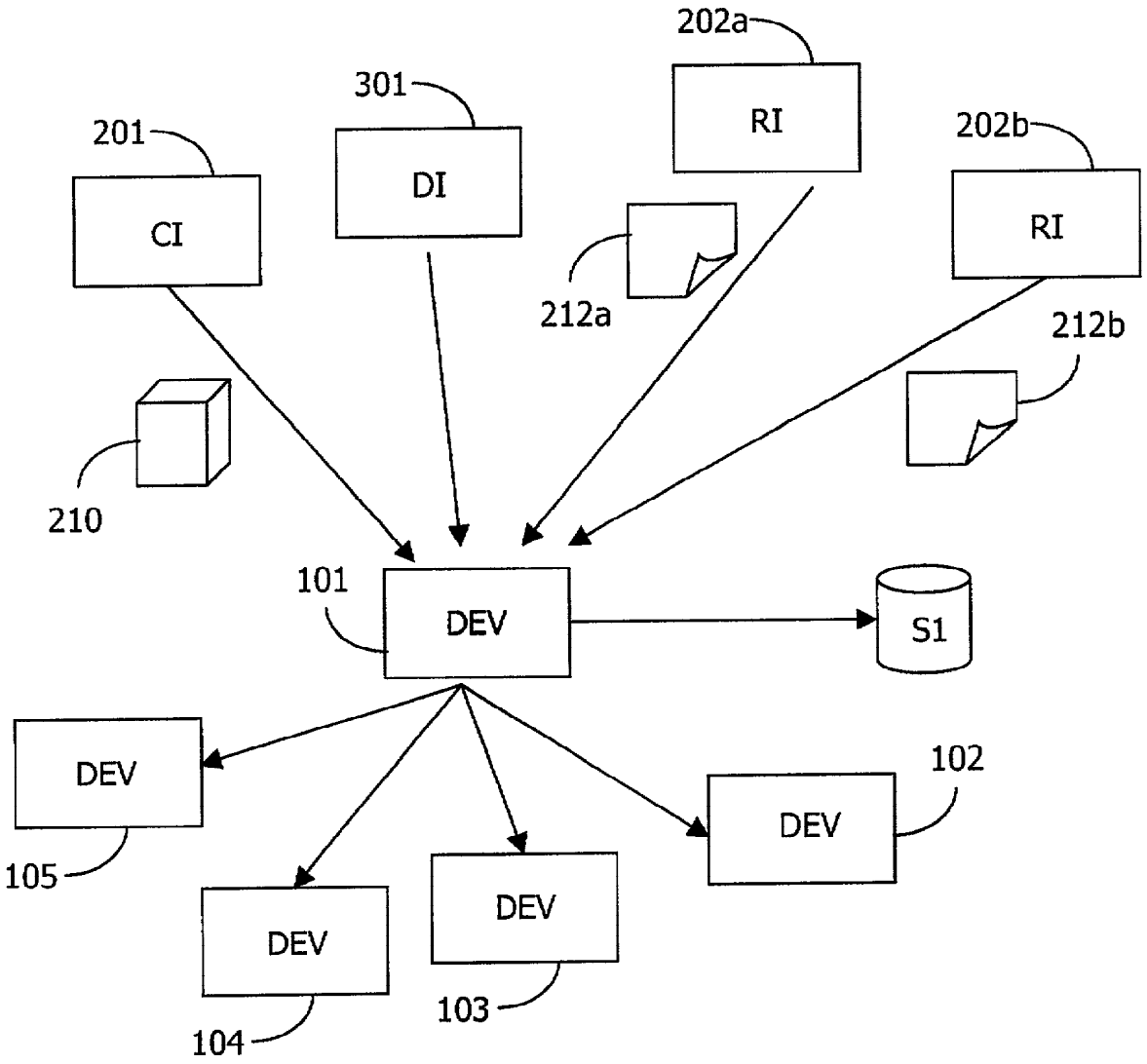
(57) Реферат:

Изобретение относится к области защиты контента. Техническим результатом является расширение функциональных возможностей доступа к объектам для сущностей в домене за счет использования диверсифицированного ключа, который получается с помощью односторонней функции из общего доменного ключа. В домене, содержащем множество устройств, устройства в домене совместно используют общий доменный ключ, способ предоставления возможности сущности, которая не является членом домена, создавать объект, который может быть аутентифицирован и/или дешифрован с помощью общего доменного ключа, способ содержит этап предоставления сущности, которая не является членом домена, диверсифицированного ключа, который выводится с помощью односторонней функции, по меньшей мере, из общего доменного ключа, для создания данных аутентификации, относящихся к упомянутому объекту, и/или для шифрования упомянутого объекта, устройства в домене конфигурируются так, чтобы аутентифицировать и/или дешифровать упомянутый объект с помощью

RU 2447498 C2

RU 2447498 C2

диверсифицированного ключа. 3 н. и 9 з.п. ф- лы, 3 ил.



ФИГ. 3

RU 2447498 C2

RU 2447498 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 447 498** (13) **C2**

(51) Int. Cl.
G06F 21/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2008147396/08, 25.04.2007**

(24) Effective date for property rights:
25.04.2007

Priority:
(30) Priority:
02.05.2006 EP 06113373.2

(43) Application published: **10.06.2010** Bull. 16

(45) Date of publication: **10.04.2012 Bull. 10**

(85) Commencement of national phase: **02.12.2008**

(86) PCT application:
IB 2007/051533 (25.04.2007)

(87) PCT publication:
WO 2007/125486 (08.11.2007)

Mail address:
129090, Moskva, ul. B. Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. A.V.Mitsu, reg. №364

(72) Inventor(s):
KOSTER Robert P. (NL),
MONTANER Khav'er (NL),
JaKOB Sorin M. (NL),
KORAJKhI Najib (NL)

(73) Proprietor(s):
KONINKLEJKE FILIPS EhLEKTRONIKS N.V. (NL),
VODAFON LIBERTEL B.V. (NL),
STIKhTING TELEMATIKA INSTIT'JuT (NL)

RU 2447498 C2

(54) IMPROVED ACCESS TO DOMAIN

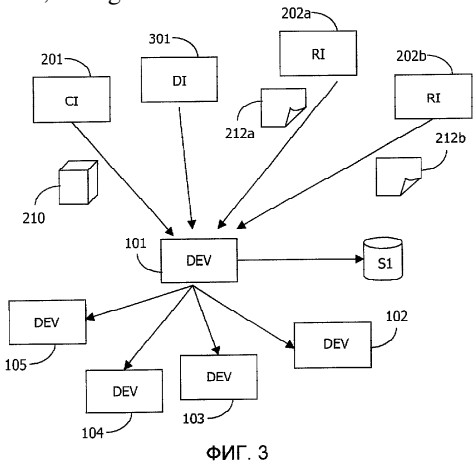
(57) Abstract:

FIELD: information technology.

SUBSTANCE: in domain containing multiple devices, the devices in domain shares common domain key, method of enabling an entity which is not domain member to create an object which can be authenticated and/or decoded using common domain key, the method contains step of providing an entity which is not domain member with diversified key which is produced using one-sided function form at least common domain key to create authentication data relating to the mentioned object and/or to encrypt the mentioned object, devices in the domain are configured so that the mentioned object could be authenticated and/or encoded using diversified key.

EFFECT: enhancement of functionality of access to objects for entities in domain due to use of diversified key which is obtained using one-sided function from common domain key.

12 cl, 3 dwg



ФИГ. 3

RU 2447498 C2

УРОВЕНЬ ТЕХНИКИ ИЗОБРЕТЕНИЯ

В последние годы число доступных систем защиты контента быстро увеличивалось. Некоторые из этих систем защищают контент только от неавторизованного копирования, тогда как другие ограничивают возможность пользователя осуществлять доступ или использовать контент. Эти системы часто упоминаются как системы управления цифровыми правами (DRM).

Потребители хотят наслаждаться контентом без сложностей и с минимально возможными ограничениями. Они хотят объединять свои устройства в сеть, чтобы обеспечить все типы различных приложений и легко осуществлять доступ ко всем типам контента. Они также хотят иметь возможность совместно использовать/переносить контент в домашнем окружении без ограничений.

Концепция авторизованных доменов (AD) нацеливается на поиск решения для того, чтобы удовлетворить интересы как владельцев контента (которые хотят защитить свои авторские права), так и потребителей контента (которые хотят неограниченного использования контента). Основной принцип заключается в том, чтобы иметь управляемое сетевое окружение, в котором контент может быть использован относительно свободно, пока он не пересечет границу авторизованного домена. Типично, авторизованные домены сконцентрированы вокруг домашнего окружения, также именуемого как домашние сети.

Конечно, другие контексты также возможны. Пользователь может, например, взять переносное устройство для аудио и/или видео с ограниченным количеством контента с собой в поездку и использовать его в своей комнате в гостинице для того, чтобы получить доступ или загрузить дополнительный контент, сохраненный в своей персональной аудио- и/или видеосистеме дома. Даже если переносное устройство находится за пределами домашней сети, оно является частью авторизованного домена пользователя. В таком способе авторизованный домен (AD) является системой, которая позволяет осуществлять доступ к контенту посредством устройств в домене, но не каких-либо других.

Авторизованным доменам необходимо разрешить проблемы, такие как идентификация авторизованного домена, проверка устройства на входе, проверка устройства на выходе, проверка прав на входе, проверка прав на выходе, проверка контента на входе, проверка контента на выходе, так же как и управление доменом. Для более обширного введения в использование авторизованного домена и т.д. см. S.A.F.A van den Heuvel, W.Jonker, F.L.A.J. Kamperman, P.J. Lenoir, Secure Content Management in Autorised Domains, Philips Research, The Netherlands, публикация конференции IBC 2002, страницы 467-474, сохраненную 12-16 сентября 2002 г.

В определенных архитектурах авторизованных доменов сущности, например, устройства, в домене совместно используют симметричный доменный ключ, который используется, среди прочего, для того, чтобы создавать, обращаться и/или аутентифицировать объекты, такие как контент или лицензии (объекты прав), которые доступны в домене. Одним примером является версия 2 DRM-архитектуры открытого сообщества производителей мобильной связи: утвержденная версия 2.0, OMA-AD-DRM-V2_0-20060303-A, 3 марта 2006 года, далее в данном документе называемая OMA DRM v2 для краткости. Этот документ доступен в Интернете по адресу и содержится по ссылке в настоящем документе. Другим примером является WO 2005/088896 (адвокатская выписка PHNL040288).

В таких архитектурах доменный ключ не может быть сделан доступным сущностям, не являющимся членами, так как это позволит им обращаться к

защищенным объектам, даже если они не являются членами домена. Однако желательно, чтобы определенным сущностям, не являющимся членами, было разрешено создавать объекты для использования сущностями в домене. Можно, конечно, выдать этим сущностям, не являющимся членами, разные ключи, но это требует того, чтобы каждое устройство в каждом домене сохраняло копии всех этих ключей.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

Целью изобретения является предоставление возможности для сущности, которая не является членом авторизованного домена, создавать объекты, которые используются членами авторизованного домена, без предоставления этой сущности доменного ключа.

Эта цель достигается в способе по пункту 1 формулы. Предоставляя устройству или другой сущности, которая не является членом домена, диверсифицированный ключ, который получается с помощью односторонней функции из общего доменного ключа, для этого устройства становится возможным создавать данные аутентификации, относящиеся к этим объектам, и/или шифровать эти объекты с помощью диверсифицированного ключа. Устройства в домене могут создавать диверсифицированный ключ, когда необходимо, получая его с помощью односторонней функции из доменного ключа, который доступен им. Они могут затем использовать диверсифицированный ключ, чтобы аутентифицировать и/или дешифровать объекты, принятые от сущности, не являющейся членом.

Согласно изобретению сущность, не являющаяся членом, не имеет доступа к доменному ключу, хотя она способна создавать объекты, которые могут быть аутентифицированы и/или дешифрованы устройствами в домене. Это обеспечивает лучшее управление, при котором сущности могут выдавать такие объекты, например объекты прав OMA DRM, домену.

Предпочтительно диверсифицированный ключ получается с помощью односторонней функции из общего доменного ключа и из представления идентичности сущности, которая не является членом домена. Это имеет преимущество в том, что разные сущности принимают разные диверсифицированные ключи.

В предпочтительном варианте осуществления односторонняя функция содержит снабженную ключом криптографическую хэш-функцию. В качестве входных данных в этой функции можно использовать представление идентичности сущности, которая не является членом домена, например, открытый ключ, ассоциативно связанный с устройством. Когда алгоритм аутентификации или шифрования требует, чтобы ключи были конкретной длины, можно обрезать выходные данные односторонней функции до требуемого числа битов. Например, при использовании диверсифицированного ключа с алгоритмом AES-шифрования, использующего 128-битные ключи, ключ, сформированный с помощью SHA-1 односторонней хэш-функции, должен быть обрезан со 160 до 128 битов.

В предпочтительном варианте осуществления сущность, не являющаяся членом, является издателем прав, сконфигурированным для выдачи цифровых прав, ассоциативно связанных с элементами контента. В этом варианте осуществления объекты, содержащие цифровые права, шифруются с помощью диверсифицированных ключей.

В варианте осуществления способ дополнительно содержит создание подписанного цифровым образом маркера действительности, содержащего представление идентичности сущности, которая не является членом домена.

В дополнительном варианте осуществления способ содержит создание кода аутентификации сообщения для объектов, предоставленных сущностью, которая не является членом домена, с помощью общего доменного ключа. Устройства, которые принимают такой объект от другого устройства, теперь также требуют присутствия действительного кода аутентификации сообщения. Это не позволяет сущности, не являющейся членом, формировать действительные объекты для конкретного домена и делать их доступными через различные каналы.

Изобретение дополнительно предоставляет систему и устройство для выполнения способа.

Другие преимущественные варианты осуществления излагаются в зависимых пунктах формулы изобретения.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Эти и другие аспекты изобретения будут видны из и объяснены со ссылкой на иллюстративные варианты осуществления, показанные на чертежах, на которых:

Фиг.1 схематично иллюстрирует систему, содержащую устройства, соединенные между собой посредством сети;

Фиг.2 показывает схематическую архитектуру согласно стандарту OMA DRM v2, и

Фиг.3 показывает схематическую архитектуру согласно изобретению, содержащую отдельного доменного издателя и множество издателей прав.

На всех чертежах одинаковые номера ссылок указывают аналогичные или соответствующие признаки. Некоторые из признаков, указываемых на чертежах, в типичном варианте реализуются в программном обеспечении и, по сути, представляют программные объекты, такие как программные модули или объекты.

ПОДРОБНОЕ ОПИСАНИЕ ВАРИАНТОВ ОСУЩЕСТВЛЕНИЯ

Фиг.1 схематично иллюстрирует систему 100, содержащую устройства 101-105, соединенные между собой через сеть 110. Типичная цифровая домашняя сеть включает в себя ряд устройств, к примеру, приемное радиоустройство, тюнер/декодер, CD-проигрыватель, пару громкоговорителей, телевизор, VCR или цифровой рекордер, мобильный телефон, магнитофон, персональный компьютер, персональное цифровое устройство, портативное устройство отображения, автомобильную развлекательную систему и т.п. Эти устройства обычно соединены между собой, чтобы предоставить возможность одному устройству, к примеру, телевизору, управлять другим, к примеру, VCR. В некоторых вариантах осуществления, одно устройство, такое как, к примеру, тюнер/декодер или телевизионная абонентская приставка (STB), функционирует как центральное устройство, предоставляющее централизованное управление над другими устройствами.

Содержимое, которое в типичном варианте содержит, например, музыку, песни, фильмы, анимацию, речь, видеоклипы для музыки, ТВ-программы, изображения, игры, мелодии звонков, голосовые книги и т.п., но также может включать в себя интерактивные службы, принимается через различные источники, такие как широковещательная кабельная сеть, Интернет-соединение, спутниковая нисходящая линия связи, сети мобильных телефонов, носители хранения типа дисков или переносных устройств. Контент далее может переноситься по сети 110 в приемник для подготовки посредством рендеринга. Приемником может быть, например, телевизионный дисплей 102, портативное устройство 103 отображения, мобильный телефон 104 и/или устройство 105 воспроизведения аудио.

Точный способ, которым элемент контента подготавливается посредством рендеринга, зависит от типа устройства и типа контента. Например, в приемном

радиоустройстве подготовка посредством рендеринга содержит формирование аудиосигналов и их подачу в громкоговорители. Для телевизионного приемного устройства подготовка посредством рендеринга, в общем, содержит формирование аудио- и видеосигналов и их подачу на экран отображения и громкоговорители. Для других типов контента должно быть выполнено аналогичное соответствующее действие. Подготовка посредством рендеринга также может включать в себя такие операции, как расшифровку или дескремблирование принимаемого сигнала, синхронизацию аудио- и видеосигналов и т.п.

Телевизионная абонентская приставка 101 или любое другое устройство в системе 100 может содержать носитель хранения S1, такой как жесткий диск подходящего объема, предоставляющий возможность записи и последующего воспроизведения принимаемого контента. Носителем хранения S1 может быть персональный цифровой рекордер (PDR) определенного типа, например рекордер DVD+RW, к которому подсоединена телевизионная абонентская приставка 101. Контент также может поступать в систему 100 сохраненным на носителе 120, таком как компакт-диск (CD) или универсальный цифровой диск (DVD).

Портативное устройство 103 отображения и мобильный телефон 104 подключаются беспроводным способом к сети 110 с помощью базовой станции 111, например с помощью Bluetooth или IEEE 802.11b. Другие устройства подключаются с помощью традиционного проводного соединения. Чтобы дать возможность устройствам 101-105 взаимодействовать, доступно несколько стандартов взаимодействия, которые позволяют различным устройствам обмениваться сообщениями и информацией и управлять друг другом. Один хорошо известный стандарт - это стандарт универсального способа "включай-и-работай" (http://www.upnp.org).

Система 100 установлена, чтобы управлять доступом к контенту, работая как авторизованный домен (AD), предпочтительно в соответствии со стандартом OMA DRM v2 или его преемником. Фиг.2 показывает схематическую архитектуру согласно стандарту OMA DRM v2.

На фиг.2 издатель 201 содержимого (CI) создает контент 210, доступный в защищенной форме ("DRM-содержимое" в терминологии OMA) устройствам в AD, здесь устройству 101. Чтобы обратиться к контенту 210, устройству 101 необходим объект 212 прав (RO), который предоставляется издателем 202 прав (RI). Предоставление RO 212 может происходить одновременно с предоставлением DRM-контента 210, но это необязательно. Например, можно получить контент в определенное время, и позднее приобрести RO, чтобы получить доступ к этому контенту. Альтернативно можно получить RO и только позже получить контент, к которому применяется RO.

В OMA DRM RO является XML-документом, определяющим разрешения и ограничения, ассоциативно связанные с частью DRM-контента. DRM-контент не может использоваться без ассоциативно связанного RO и может использоваться только согласно разрешениям и ограничениям, определенным в RO. RO содержат выражения прав и ключи, необходимые для рендеринга фактического контента. Приобретение RO, регистрация устройства и управление доменом определяется посредством набора протоколов, названного ROAP.

Каждое из устройств 101-105 имеет DRM-агента, обычно осуществленного как компонент программного обеспечения, выполняемый в рассматриваемом устройстве. DRM-агент гарантирует, что разрешения и ограничения, определенные в RO, соблюдаются. Объект прав криптографически привязан к конкретному DRM-агенту,

так что только этот DRM-агент может использовать его.

DRM-контент 210 может свободно распространяться между устройствами 101-105 и может также быть сохранен, например, на носителе S1 хранения или распространяться другим сторонам. Однако без действительного RO доступ к DRM-контенту 210 не может быть осуществлен. Если устройство 105 должно получить копию DRM-контента 210, например, оно должно, тем не менее, получить RO, который должен быть привязан к своему DRM-агенту. RO 212 используется только DRM-агентом устройства 101.

Чтобы создать доменный доступ к контенту, OMA DRM также разрешает создание и распределение объектов прав, которые привязаны скорее к группе DRM-агентов, чем к одному агенту. Такая группа упоминается как домен, а объекты прав, привязанные к домену, упоминаются как объекты прав домена. Чтобы присоединиться к домену, первое устройство 101 должно спросить издателя 202 прав, разрешено ли присоединиться к домену. Если устройству 101 разрешено присоединиться, RI 202 предоставит устройству 101 контекст домена (DC). DC содержит доменные ключи, которые могут использоваться, чтобы дешифровать объекты прав домена. Подробнее см. секцию 6.4 спецификации OMA DRM v2.

Спецификации OMA DRM дополнительно определяют формат и механизм защиты DRM-контента, формат (язык выражений) и механизм защиты объектов прав и модель безопасности для управления ключами шифрования. Спецификации OMA DRM также определяют, как DRM-контент и объекты прав могут быть перенесены устройствам с помощью ряда транспортных механизмов, включающих в себя выталкивание из стека (HTTP-выталкивание, OMA-загрузка), помещение в стек (WAP-помещение в стек, MMS) и потоковую передачу. Передача RO использует 1-проходный или 2-проходный протокол, называемый протоколом получения объекта прав (ROAP), который выполняется между RI и DRM-агентом пользователя. Альтернативно перемещение RO может выполняться без выполнения ROAP между двумя DRM-агентами пользователя или между RI и DRM-агентом пользователя.

Отметим, что издатель 201 контента и издатель 202 прав может быть одной и той же сущностью. В терминологии OMA эта сущность тогда называется распространителем контента.

Изобретатели настоящего изобретения поняли, что существует необходимость в дополнительном разделении выдачи прав и управления доменом в OMA-решении. Главным недостатком вышеописанной архитектуры является то, что домены не могут легко использоваться совместно или использоваться между разными RI.

В соответствии с настоящим изобретением вводится отдельный доменный издатель (DI). Устройства, которые хотят присоединиться к домену, теперь связываются с DI вместо RI. В результате, множество RI могут теперь использоваться, чтобы предоставлять доменные RO одному и тому же домену. Это схематически иллюстрировано на фиг.3. Предоставлены два RI 202a, 202b, оба выдают доменные RO 212a, 212b устройству 101. Кроме того, доменный издатель (DI) 301 управляет тем, какие устройства присоединяются и покидают домен.

Доменный ключ, далее в данном документе сокращенный как K_D, теперь предоставляется посредством DI 301 вместо RI 202 устройствам 101-105. RI 202a, 202b больше не имеют доступа к доменному ключу. Это будет означать, что они больше не могут выдавать объекты прав домена устройствам 101-105, так как согласно OMA DRM v2 объекты прав домена должны быть защищены с помощью доменного ключа.

Согласно изобретению каждый RI выпускает свой собственный

диверсифицированный ключ, далее в данном документе сокращенный как K_{Di}, где i является идентификатором RI, которому выпущен диверсифицированный ключ K_{Di}. Диверсифицированный ключ получается из доменного ключа, предпочтительно вместе с идентичностью рассматриваемого издателя прав.

В предпочтительном варианте осуществления диверсифицированный ключ создается посредством вычисления снабженного ключом хэш-кода аутентификации сообщения (HMAC) представления идентичности, предпочтительно открытого ключа, издателя прав с помощью доменного ключа в качестве секретного ключа. Предпочтительно используется SHA1 криптографическая хэш-функция, хотя многие другие хэш-функции могут также использоваться. Вычисленный снабженный ключом хэш предпочтительно обрезается, чтобы сохранить только первые 128 битов, эти 128 битов затем служат в качестве диверсифицированного ключа.

Альтернативно криптографическая хэш-функция может использоваться, чтобы вычислить хэш доменного ключа, этот хэш затем служит в качестве диверсифицированного ключа. Опять же хэш может быть обрезан, если необходимо. Предпочтительно входными данными криптографической хэш-функции является не только доменный ключ, но также представление идентичности, предпочтительно открытый ключ, издателя прав. Этот предпочтительный вариант осуществления обеспечивает различные RI различными ключами. Например, можно хэшировать конкатенацию доменного ключа и открытый ключ.

В другом варианте осуществления ключ K_{Di} получается как шифрование представления идентичности RI с помощью доменного ключа DK в качестве ключа шифрования. Представление идентичности RI может быть получено разными способами в зависимости от того, какой тип имен, порядковые номера и т.д. используются в осуществлении DRM-системы. Например, DM может назначить каждому RI, который может связываться с доменом, уникальную идентифицирующую метку Lb_i, которая равна точно 128 битам (16 байтам) по длине. Это может быть порядковый номер сертификата. Если метки короче, чем 16 байтов, тогда DM должен предварительно заполнить каждую метку 0-битами, вплоть до 16 байтов, чтобы сформировать Lb_i.

Одним вариантом, чтобы создать диверсифицированный ключ, теперь является AES-шифрование этой метки Lb_i с помощью доменного ключа DK в качестве ключа шифрования. Преимуществом этого является то, что это очень просто, а получающиеся в результате ключи гарантированно должны быть уникальными.

Если каждый RI имеет произвольно выбранное и уникальное имя, тогда это имя может быть заполнено, чтобы создать строку правильной длины. Стандартные технологии заполнения доступны, см., например, ISO/IEC стандарт 9797. Одним предпочтительным вариантом является следующее. Сначала имя предварительно заполняется блоком, который равен 128 битам по длине и который является бинарным представлением (незаполненной) длины имени в битах. Затем результат-пост заполняется битами в значении '0' до тех пор, пока все сообщение не достигнет кратного 128 битам числа по длине. Результат может быть зашифрован с помощью AES с доменным ключом DK в качестве ключа шифрования. Это имеет преимущество в том, что произвольно выбранные имена могут использоваться посредством RI.

Многие альтернативные варианты могут быть рассмотрены. Теперь будет приведено несколько примеров. В большинстве случаев снабженная ключом MAC-функция может применяться вместо шифрования с помощью доменного ключа DK в

качестве ключа.

Чтобы получить диверсифицированный ключ K_{Di}, издатель прав в предпочтительном варианте осуществления выдает запрос доменному издателю. Если доменному издателю разрешено выдавать RO устройствам в рассматриваемом домене, доменный издатель выдает ответ, содержащий соответствующий контекст. Этот контекст содержит диверсифицированный ключ для издателя прав и, предпочтительно, также идентификаторы для доменного издателя, самого домена, время истечения срока действия (выраженное как момент времени или продолжительность от текущего времени) и, предпочтительно, маркер действительности RI, описанный ниже. Время истечения срока и маркер действительности могут принимать форму сертификата X.509v3 открытого ключа для издателя прав, который был сформирован с помощью закрытого ключа доменного издателя.

Издатель прав может теперь формировать объекты прав и использовать диверсифицированный ключ, чтобы зашифровать эти RO. Это то же самое, что и со стандартом OMA DRM v2, за исключением того, что теперь диверсифицированный ключ используется вместо доменного ключа.

Когда устройство в домене получает доменный RO от издателя прав, он создает диверсифицированный ключ для этого издателя прав и использует этот диверсифицированный ключ, чтобы дешифровать доменный RO. Для этого устройство повторяет процесс, как обрисовано выше для доменного издателя.

В варианте осуществления доменный издатель создает маркер действительности RI, который позволяет RI подтверждать, что ему разрешено выдавать доменные RO для устройств в рассматриваемом домене. Маркер действительности содержит идентичность, например, открытый ключ, издателя прав и, предпочтительно, также указание того, как долго маркер будет оставаться действительным, например, указывая дату истечения срока. Маркер действительности должен быть цифровым образом подписан посредством DI так, что его аутентичность может быть проверена.

В этом варианте осуществления устройство может использовать маркер действительности RI, чтобы получить идентичность, т.е. открытый ключ, издателя прав. Конечно, устройство не должно использовать маркер действительности RI, если цифровая подпись не может быть успешно проверена, или если маркер больше недействителен, например, если текущее время находится за пределами указанной даты истечения срока.

Согласно OMA DRM v2 издатель прав и устройство должны выполнить протокол регистрации RI перед тем, как устройство сможет принять RO от издателя прав. Выгода настоящего изобретения в том, что этого больше не требуется. Устройство в домене может также получить доменные RO от другого устройства в домене, и в этом случае не нужно регистрировать себя с помощью RI, который первоначально сформировал этот доменный RO.

В определенных интервалах доменный ключ может быть заменен новым доменным ключом. В этом случае доменный издатель должен также сформировать новые диверсифицированные ключи для всех издателей прав, которые выпустили диверсифицированные ключи, полученные из предыдущего доменного ключа. Доменный издатель должен затем предпочтительно предоставить эти новые диверсифицированные ключи этими издателям прав автоматически. Альтернативно они могут быть доставлены по запросу.

Вместо шифрования RO с диверсифицированными ключами диверсифицированные

ключи могут также использоваться, чтобы создать и проверить данные аутентификации, ассоциативно связанные с объектами прав. Можно, например, использовать диверсифицированный ключ в качестве ключа для снабженной ключом хэш-функции или функции кода аутентификации сообщения, которая должна быть применена к объекту прав. Выходные данные этой функции затем служат, чтобы аутентифицировать объекты прав.

Желательно не допустить формирование посредством RI действительных доменных RO для отдельного домена без вовлечения протокола приобретения RO (ROAP) с устройством, который является членом домена. Чтобы достичь этого, в предпочтительном варианте осуществления устройства в домене после приема RO во время ROAP вычисляют MAC устройства с помощью главного доменного мастер-ключа и присоединяют MAC устройства к доменному RO, когда они принимают такой доменный RO от RI. MAC устройства, таким образом, служит как доказательство того, что доменный RO был приобретен от авторизованного RI. Отметим, что этот подход служит также для RO, которые были созданы скорее с помощью доменного ключа, чем с помощью диверсифицированного ключа. Этот подход, таким образом, не ограничен RO, которые зашифрованы с помощью диверсифицированных ключей.

MAC устройства может быть вычислен как MAC RO с помощью доменного ключа K_D в качестве ключа. Это позволяет любому устройству в домене установить аутентичность MAC устройства. MAC устройства должен сопровождать RO, предпочтительно, добавляя его как новый XML-элемент в доменный RO.

В этом варианте осуществления MAC устройства требуется для последующего RO-обмена устройство-устройство и установки в устройстве назначения. Всякий раз, когда устройство принимает доменный RO, это устройство должно сначала проверить достоверность MAC устройства перед приемом и/или установкой доменного RO в устройстве.

Отметим, что после того, как доменный ключ K_D изменяется, MAC устройства больше не может быть проверен на достоверность с помощью нового доменного ключа. И доменный RO без действительного сопровождающего MAC устройства должен предпочтительно быть отвергнут устройствами в домене. Альтернативно, устройство, которое приняло и установило доменный RO с действительным MAC устройства, может повторно вычислить MAC устройства с помощью нового доменного ключа.

Безопасность решения, предложенного выше, основана на том предположении, что доменный ключ K_D известен только устройствам, которые являются членами домена, и доменному издателю. Однако если доменный ключ K_D почему-то становится доступным неавторизованной третьей стороне, для RI становится возможным выдавать доменные RO даже после того, как авторизация для этого истекла.

Чтобы решить эту проблему, устройство, которое формирует MAC устройства, должно сформировать цифровую подпись с помощью своего закрытого ключа для этого MAC устройства. Эта подпись, DeviceSign, будет распространяться вместе с доменным RO и MAC устройства. DeviceSign позволяет другим устройствам в домене идентифицировать устройство, которое приняло доменный RO от RI.

Если впоследствии доменный ключ K_D становится скомпрометированным, и выдаются неавторизованные RO, доменное устройство, которое принимает эти RO, может быть идентифицировано. Это устройство тогда вероятно действует в сговоре с неавторизованным RI. Рассматриваемое устройство может впоследствии быть аннулировано, например, посредством добавления идентификатора этого устройства

в список аннулированных устройств (DRL), который распространяется всем устройствам в домене. Законопослушные устройства принимают и устанавливают только те доменные RO, которые включают в себя соответствующую DeviceSign, сформированную устройством, которое не включено в DRL.

Чтобы поддерживать вышеизложенное, доменный издатель в предпочтительном варианте осуществления формирует подписанный объект, который информирует каждое устройство в домене о том, что отдельному устройству, далее в данном документе $device_x$, разрешено создавать подписи DeviceSign. Маркер содержит открытый ключ $device_x$ и подписан посредством DI так, что он может быть проверен на достоверность любым устройством-членом домена. Предпочтительно, маркер сделан доступным для $device_x$, так что это устройство может распространять его другим устройствам.

В этом варианте осуществления всякий раз, когда устройство принимает доменный RO, ему нужно выполнять проверку действительности DeviceSign и маркера для $device_x$ в дополнение к другим, уже рассмотренным этапам.

В этом варианте осуществления дополнительно каждое устройство в домене имеет доступ к списку аннулированных устройств, DRL, для устройств в домене. Этот DRL может быть сохранен в устройствах или, например, быть доступен через сеть. DRL предпочтительно реализован как черный список посредством перечисления устройств, чьи DeviceSign не должны быть приняты. Альтернативно, DRL может быть реализован как белый список посредством перечисления только тех устройств, чьи DeviceSign должны быть приняты.

Изобретение также может использоваться, чтобы защитить и/или аутентифицировать другие объекты, отличные от объектов прав. Например, контент может быть зашифрован с помощью диверсифицированных ключей.

Изобретение применяется не только к доменам в соответствии с OMA DRM. Существуют различные предложения, которые в некоторой степени осуществляют концепцию авторизованных доменов. В так называемых AD на основе устройств домен формируется посредством конкретного набора аппаратных устройств или приложений системы программного обеспечения (далее в данном документе собирательно называемых клиенты) и контента. Менеджер домена, которым может быть одним или более клиентом, смарт-картой или другим устройством, управляет тем, какие клиенты могут присоединяться к домену. Только конкретному набору клиентов в домене (членам) разрешено использовать контент этого домена, например, открывать, копировать, воспроизводить или экспортировать его. Примеры таких AD на основе устройств даны в международной патентной заявке WO 03/098931 (адвокатская выписка PHNL020455), международной патентной заявке WO 05/088896 (адвокатская выписка PHNL040288) и международной патентной заявке WO 04/027588 (адвокатская выписка PHNL030283) того же заявителя, все из которых содержатся в данном документе по ссылке.

Один тип AD на основе устройств позволяет набору клиентов, прикрепленных к домену, обращаться к контенту, прикрепленному к этому домену. Эта двойная привязка гарантирует то, что все члены могут обращаться к контенту. Эта структура часто устанавливается посредством осуществления привязок через совместно используемый секретный ключ. Этот ключ выбирается менеджером домена и распространяется всем членам. Когда контент привязан к домену, лицензия криптографически ссылается на домен посредством шифрования с помощью совместно используемого ключа. Альтернативно, контент может быть

непосредственно привязан к одному клиенту, а клиенты остаются привязанными к AD.

Другим типом AD является так называемый AD на основе человека, где домен основан на людях вместо устройств. Пример такой системы описан в международной патентной заявке WO 04/038568 (адвокатская выписка PHNL021063) того же заявителя, содержащейся в данном документе по ссылке, в которой контент связывается с людьми, которые затем группируются в домен.

Так называемая DRM-система на основе гибридного авторизованного домена связывает контент в группы, которые могут содержать устройства и людей. Эта группа типично ограничена семейством так, что:

1) контент может просматриваться любым из членов, который принадлежит семейству (например, ТВ в комнате, ТВ в ванной, ПК);

2) контент может быть просмотрен любым из пользователей, которые принадлежат семейству после того, как они аутентифицировали себя на любом клиенте (таком как телевизор в комнате в гостинице). Такая аутентификация обычно затрагивает устройство аутентификации пользователя, такое как смарт-карта.

Примеры гибридных AD-систем могут быть найдены в международной патентной заявке WO 2005/010879 (адвокатская выписка PHNL030926) и международной патентной заявке WO 2005/093544 (адвокатская выписка PHNL040315), обе содержатся в данном документе по ссылке.

Международная патентная заявка порядковый номер PCT/IB2005/053531 (адвокатская выписка PHNL041254) описывает способ разрешения доступа к авторизованному домену, авторизованный домен управляется менеджером домена, содержащий этап, на котором устройство аутентификации пользователя, причем это устройство аутентификации пользователя ссылается на чужое устройство, заявляет менеджеру домена, что линия внутренней связи между устройством аутентификации пользователя и чужим устройством ограничена по расстоянию, и этап, на котором менеджер домена разрешает чужому устройству работать как члену авторизованного домена, если утверждение принимается как правильное.

Международная патентная заявка порядковый номер PCT/IB2005/053687 (адвокатская выписка PHNL041329) описывает систему авторизованного домена, содержащую множество устройств, включающих в себя, по меньшей мере, одно поисковое устройство, при этом поисковое устройство сконфигурировано, чтобы отыскивать информацию о состоянии аннулирования для двух или более устройств, содержащихся в домене, и распространять найденную информацию о состоянии аннулирования одному или более устройствам, с которыми поисковое устройство находится на связи.

Международная патентная заявка WO 2004/077790 (адвокатская выписка PHFR030018) описывает телекоммуникационную систему для широковещательной передачи мультимедийного содержимого клиентскому устройству. Упомянутая система содержит кодер для кодирования упомянутого мультимедийного контента в закодированный поток данных. Упомянутый закодированный поток данных передается через первое сетевое соединение серверу. Упомянутый сервер способен формировать метаданные из мультимедийных данных, содержащихся в принятом закодированном потоке данных, и создавать прогрессивный файл, в котором упомянутые мультимедийные данные и метаданные чередуются. Упомянутый прогрессивный файл загружается через второе сетевое соединение в клиентское устройство, которое способно начать воспроизведение принятого мультимедийного контента перед окончанием загрузки с помощью

упомянутых чередующихся мета- и мультимедийных данных.

Следует отметить, что вышеуказанные варианты осуществления иллюстрируют, а не ограничивают изобретение, и специалисты в данной области техники должны иметь возможность проектировать множество альтернативных вариантов осуществления без отступления от области применения прилагаемой формулы изобретения.

В формуле изобретения все номера ссылок, помещенные в круглые скобки, не должны рассматриваться как ограничивающие формулу изобретения. Слово "содержащий" не исключает наличия элементов или этапов, не перечисленных в формуле изобретения. Использование в единственном числе не исключает наличия множества таких элементов. Изобретение может быть реализовано посредством аппаратных средств, содержащих несколько отдельных элементов, и посредством надлежащим образом запрограммированного компьютера.

В пункте формулы изобретения по устройству, перечисляющем несколько средств, некоторые из этих средств могут быть осуществлены посредством одного и того же элемента аппаратных средств. Простой факт того, что определенные меры упомянуты в различных зависимых пунктах формулы изобретения, не означает того, чтобы комбинация этих мер не может быть использована с выгодой.

Формула изобретения

1. Способ предоставления возможности сущности, которая не является членом домена и которая не имеет доступа к общему доменному ключу, создавать объект, который может быть аутентифицирован и/или дешифрован с помощью общего доменного ключа, причем домен содержит множество устройств, которые совместно используют общий доменный ключ, причем способ содержит этапы, на которых:

предоставляют сущности, которая не является членом домена, диверсифицированный ключ, который выводится с помощью односторонней функции, по меньшей мере, из общего доменного ключа, для создания данных аутентификации, относящихся к упомянутому объекту, и/или для шифрования, по меньшей мере, части упомянутого объекта, и

аутентифицируют и/или дешифруют упомянутый объект с помощью диверсифицированного ключа.

2. Способ по п.1, в котором односторонняя функция содержит снабженную ключом криптографическую хэш-функцию.

3. Способ по п.2, в которой входные данные, используемые в упомянутой снабженной ключом криптографической хэш-функции, содержат представление идентичности сущности, которая не является членом домена, а используемый ключ является общим доменным ключом.

4. Способ по п.1, в котором диверсифицированный ключ выводится посредством усечения выходных данных односторонней функции до предопределенного числа битов.

5. Способ по п.1, дополнительно содержащий этап, на котором создают подписанный цифровым образом маркер действительности, содержащий представление идентичности сущности, которая не является членом домена.

6. Способ по п.1, дополнительно содержащий этап, на котором создают код аутентификации сообщения для объектов, предоставленных сущностью, которая не является членом домена, с помощью общего доменного ключа.

7. Способ по п.1, в котором объекты содержат цифровые права для контента, к которому осуществляется доступ.

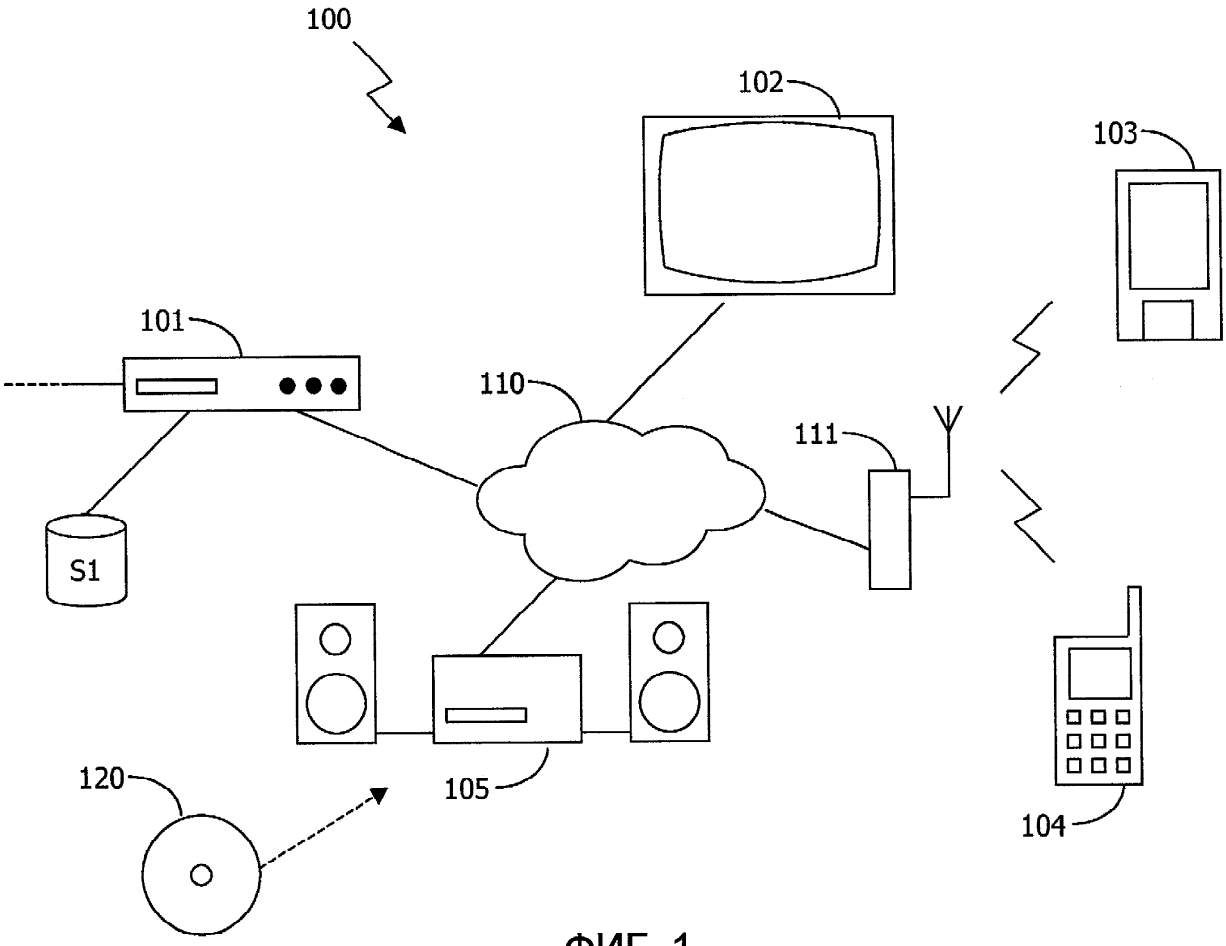
8. Способ по п.1, содержащий этап, на котором выводят диверсифицированный ключ с помощью односторонней функции из общего доменного ключа и из представления идентичности сущности, которая не является членом домена.

9. Система для защиты контента, содержащая домен, содержащий множество устройств, причем устройства в домене совместно используют общий доменный ключ, при этом система конфигурируется для предоставления возможности сущности, которая не является членом домена и которая не имеет доступа к общему доменному ключу, создавать объект, который может быть аутентифицирован и/или дешифрован с помощью общего доменного ключа посредством предоставления сущности, которая не является членом домена, диверсифицированного ключа, который получается с помощью односторонней функции, по меньшей мере, из общего доменного ключа, для создания данных аутентификации, относящихся к упомянутому объекту и/или для шифрования упомянутого объекта, при этом устройства в домене конфигурируются так, чтобы аутентифицировать и/или дешифровать упомянутый объект с помощью диверсифицированного ключа.

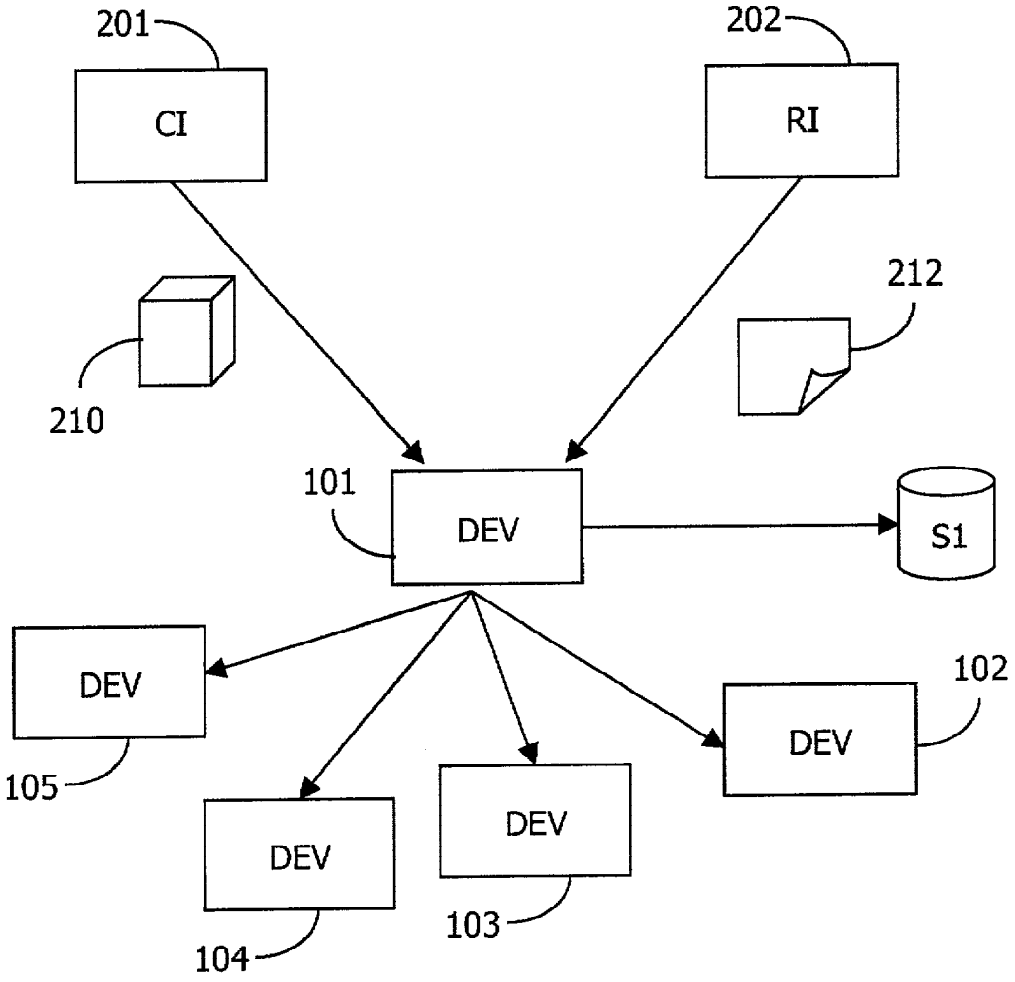
10. Устройство для защиты контента, содержащееся в домене, причем устройства в домене совместно используют общий доменный ключ, при этом устройство конфигурируется для приема объекта от сущности, которая не является членом домена и которая не имеет доступа к общему доменному ключу, для выведения диверсифицированного ключа с помощью односторонней функции, по меньшей мере, из общего доменного ключа и для аутентификации и/или дешифрования объекта с помощью диверсифицированного ключа.

11. Устройство по п.10, конфигурируемое для вычисления кода аутентификации сообщения для объекта с помощью общего доменного ключа и для распространения объекта другому устройству в домене вместе с вычисленным кодом аутентификации сообщения.

12. Устройство по п.11, конфигурируемое для приема нового общего доменного ключа, вычисления нового кода аутентификации сообщения для объекта с помощью нового общего доменного ключа и для распространения объекта другому устройству в домене вместе с вычисленным кодом аутентификации сообщения.



ФИГ. 1


201
CI
202
RI
212
210
101
DEV
S1
DEV
105
DEV
102
DEV
DEV
104
DEV
103

ФИГ. 2