РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 367 014** (13) **C2**

(51) МПК
G06F 21/22 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2005112105/02, 22.04.2005**

(24) Дата начала отсчета срока действия патента:
22.04.2005

(30) Конвенционный приоритет:
23.04.2004 US 10/830,632

(43) Дата публикации заявки: **27.10.2006**

(45) Опубликовано: **10.09.2009** Бюл. № **25**

(56) Список документов, цитированных в отчете о поиске: **WO 01/52021 A1, 19.07.2001. SU 746742 A, 05.07.1980. RU 2067313 C1, 27.09.1996. RU 2152074 C1, 27.06.2000. RU 27432 U1, 27.01.2003.**

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):
КАТТЕР Бенджамин Брукс (US),
ЭВАНС Брайан П. (US),
СТРОМ Клиффорд П. (US),
ПАРКС Майкл Джей (US)

(73) Патентообладатель(и):
МАЙКРОСОФТ КОРПОРЕЙШН (US)

(54) ОПРЕДЕЛЕНИЕ СТЕПЕНИ ДОСТУПА К СОДЕРЖИМОМУ И ТОМУ ПОДОБНОМУ В СИСТЕМЕ ЗАЩИТЫ СОДЕРЖИМОГО ИЛИ ТОМУ ПОДОБНОГО

(57) Реферат:

Способ передачи накопленных измеренных данных от клиента в службу измерений, причем каждый набор измеренных данных индексируется в базе данных измерений клиента в соответствии с идентификатором измерений (MID) и дополнительно индексируется в базе данных измерений в соответствии с идентификатором, ассоциированным с содержимым (KID). Для повышения эффективности защиты баз данных от несанкционированного доступа клиент выбирает конкретный идентификатор MID, выбирает, по меньшей мере, часть измеренных данных в базе данных измерений, содержащих выбранный идентификатор MID, где выбранные измеренные данные упорядочены в соответствии с идентификатором KID, формирует запрос на основе выбранных измеренных данных, посылает сформированный запрос в службу измерений. При этом служба измерений получает измеренные данные из запроса, сохраняет их и формирует ответ, который должен быть возвращен клиенту на основании запроса, клиент получает ответ из службы измерений, включающий в себя список идентификаторов KID выбранных данных измерений в запросе, подтверждает, что ответ соответствует запросу, и обрабатывает список идентификаторов KID в ответе путем, для каждого идентификатора KID, удаления измеренных данных из базы данных измерений, содержащих выбранные идентификаторы MID и KID. 2 н. и 18 з.п. ф-лы, 4 ил.

RU 2367014 C2

RU 2367014 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 367 014** (13) **C2**

(51) Int. Cl.
G06F 21/22 (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2005112105/02, 22.04.2005**

(24) Effective date for property rights:
22.04.2005

(30) Priority:
23.04.2004 US 10/830,632

(43) Application published: **27.10.2006**

(45) Date of publication: **10.09.2009 Bull. 25**

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):
KATTER Bendzhamin Bruks (US),
EhVANS Brajan P. (US),
STROM Klifford P. (US),
PARKS Majkl Dzhej (US)

(73) Proprietor(s):
MAJKROSOFT KORPOREJShN (US)

(54) DETERMINATION OF DEGREE OF ACCESS TO CONTENT OR SIMILAR IN SYSTEM FOR PROTECTING CONTENT OR SIMILAR

(57) Abstract:

FIELD: physics; computer engineering.

SUBSTANCE: method of transferring accumulated measured data from a client to a measurement service, where each set of measured data is indexed in the measured data base of the client in accordance with a measurement identifier (MID) and further indexed in the measurement data base in accordance with an identifier, associated with content (KID). To increase effectiveness of protecting the data base from unauthorised access, the client chooses a specific MID, chooses at least part of measured data in the measurement data base, containing the chosen MID, where the chosen measured data are arranged in accordance with KID. The client generates a request based on the chosen measured data and sends the request to the measurement service. The measurement service receives measured data from the request, stores them and generates a response, which should be returned to the client based on the request. The client receives the response from the measurement service, which includes a list of KID of chosen measured data in the request, confirms that the response corresponds to the request, and generates a list of KID in response, for each KID, by deleting measured data from the measurement data base, containing the chosen MID and KID.

EFFECT: more effective protection of data base from unauthorised access.

20 cl, 4 dwg

RU 2367014 C2

RU 2367014 C2

Область техники

Настоящее изобретение относится к архитектуре и способу обеспечения возможности определения степени доступа к цифровому содержимому и тому подобному, особенно в контексте системы защиты содержимого. Более конкретно, настоящее изобретение относится к такой архитектуре и способу, в которых данные, представляющие оцененную степень доступа к содержимому, накапливаются и сообщаются в службу определения степени доступа.

Предшествующий уровень техники

Как известно, и как показано на фиг.1, система защиты содержимого и обеспечения законного его использования является в высшей степени желательной в связи с цифровым содержимым 12, таким как цифровое аудио, цифровое видео, цифровой текст, цифровые данные, цифровые мультимедийные данные и т.д., где такое цифровое содержимое 12 должно предоставляться пользователям. После получения пользователем такого цифрового содержимого пользователь воспроизводит или «проигрывает» цифровое содержимое с помощью подходящего устройства воспроизведения, такого как мультимедийное устройство воспроизведения на персональном компьютере 14, портативное устройство воспроизведения и т.д.

В типовом случае владелец содержимого, распространяющий такое цифровое содержимое 12, желает ограничить действия пользователя в отношении такого распространяемого цифрового содержимого 12. Например, владельцу содержимого может быть желательным запретить копирование и предоставление такого содержимого 12 второму пользователю, или он может разрешить воспроизведение распространяемого цифрового содержимого 12 только ограниченное число раз, или только в течение некоторого суммарного времени, или на машине определенного типа, или на мультимедийном устройстве воспроизведения определенного типа, или пользователем определенного типа и т.п.

Однако после того как распространение содержимого состоялось, подобный владелец содержимого имеет весьма незначительные возможности контроля цифрового содержимого 12, если только вообще имеет такие возможности. В этом случае система 10 защиты от копирования обеспечивает возможность контролируемого воспроизведения или проигрывания произвольных форм цифрового содержимого 12, причем такой контроль является гибким и может определяться владельцем данного цифрового содержимого. В типовом случае содержимое распространяется пользователю в форме упаковки 13 посредством подходящего канала распространения. Упаковка 13 цифрового содержимого, используемая для его распространения, может включать в себя цифровое содержимое 12, зашифрованное с использованием симметричного ключа шифрования/дешифрования (KD) (т.е. (KD(содержимое))), а также другую информацию, идентифицирующую содержимое, как приобрести лицензию на такое содержимое и т.д.

Основанная на доверительных отношениях сстема 10 защиты от копирования позволяет владельцу цифрового содержимого определить правила, которые должны быть удовлетворены, прежде чем такое цифровое содержимое 12 будет разрешено воспроизвести. Такие правила включают в себя вышеуказанные и/или другие подобные требования и могут быть воплощены в цифровой лицензии 16, которую пользователь/пользовательское вычислительное устройство 14 (далее эти термины используются взаимозаменяемым образом, если только определенные обстоятельства не требуют иного) должны получить от владельца содержимого или его агента, или такие правила могут уже быть присоединены к содержимому 12. Такая лицензия 16

и/или правила могут, например, включать в себя ключ дешифрования (KD) для дешифрования цифрового содержимого 12, возможно, зашифрованного в соответствии с другим ключом, который может дешифрироваться пользовательским вычислительным устройством или другим устройством воспроизведения.

Владелец части цифрового содержимого 12 предпочел бы не распространять содержимое 12 пользователю до тех пор, пока этот владелец не смог бы удостовериться, что пользователь будет соблюдать правила, определенные данным владельцем содержимого в лицензии 16 или каким-либо еще образом. При этом пользовательское вычислительное устройство или другое устройство воспроизведения предпочтительно обеспечивается доверительным компонентом или механизмом 18, который не будет воспроизводить цифровое содержимое 12 иным образом, кроме как только в соответствии с указанными правилами.

Доверительный компонент 18 в типовом случае имеет блок 20 оценки, который анализирует правила и определяет на основе анализа правил, в числе прочего, имеет ли право запрашивающий пользователь воспроизвести запрошенное цифровое содержимое 12 в том виде, как запрашивается. Понятно, что блок 20 оценки уполномочен системой 10 защиты от копирования выполнять желания владельца цифрового содержимого 12 в соответствии с указанными правилами, и пользователь не должен иметь простой возможности изменить такой доверительный компонент 18 и/или блок 20 оценки с любыми целями, нечестными или еще какими-либо.

Понятно, что правила для воспроизведения содержимого 12 могут определять, имеет ли пользователь права на воспроизведение, на основе любого из различных факторов, включая то, кем является пользователь, где находится пользователь, какой тип пользовательского вычислительного устройства или другого устройства воспроизведения использует пользователь, какое приложение воспроизведения вызывает систему 10 защиты от копирования, дату, время и т.д. Кроме того, правила могут ограничить воспроизведение, например, предварительно определенным количеством воспроизведений, предварительно определенным временем воспроизведения.

Правила могут быть определенными в соответствии с любым соответствующим языком и синтаксисом. Например, язык может просто определить атрибуты и значения, которые должны быть удовлетворены (например, дата (DATA) должна быть позже, чем X), или может потребовать выполнения функций в соответствии с определенным сценарием (например, «если дата больше, чем X, то делать…»).

После того как блок 20 оценки определяет, что правила удовлетворены, цифровое содержимое 12 может воспроизводиться. В частности, для воспроизведения содержимого 12, получают ключ дешифрования (KD) из предварительно определенного источника, такого как вышеупомянутая лицензия 16, и применяют к структуре (KD(содержимое)) из упаковки 13 содержимого для получения действительного содержимого 12, и затем действительное содержимое реально воспроизводится.

Заметим, что доверительный компонент 18 может иногда требоваться для поддержания информации состояния, релевантной для воспроизведения конкретной части содержимого 12 и/или использования конкретной лицензии 16. Например, может иметь место случай, когда конкретная лицензия 16 устанавливает требование числа воспроизведений, и соответственно доверительный компонент 18 должен помнить, сколько раз была использована лицензия 16 для воспроизведения соответствующего содержимого 12, или сколько раз лицензия может быть использована для

воспроизведения соответствующего содержимого 12. Соответственно, доверительный компонент 18 может также включать в себя, по меньшей мере, одно постоянное защищенное ЗУ 22, в котором такая информация состояния постоянно поддерживается с обеспечением защиты. Таким образом, доверительный компонент 18 хранит такую информацию состояния в таком защищенном ЗУ 22 стабильным образом, чтобы такая информация состояния поддерживалась даже в сеансах использования вычислительного устройства 14. Такое защищенное ЗУ может располагаться в вычислительном устройстве 14 доверительного компонента 18, хотя такое защищенное ЗУ альтернативно может располагаться где угодно.

В системе 10 защиты от копирования содержимое 12 скомпоновано для применения пользователем путем шифрования такого содержимого 12 и ассоциирования с содержимым 12 набора правил, причем содержимое 12 может воспроизводиться только в соответствии с указанными правилами. Поскольку содержимое 12 может воспроизводиться только в соответстии с указанными правилами, содержимое 12 может свободно распространяться. В типовом случае содержимое 12 зашифровывается в соответствии с симметричным ключом, таким как упомянутый ключ (KD) для получения в результате структуры KD (содержимое), и структура KD (содержимое) поэтому также дешифруется в соответствии с ключом (KD) для получения в результате содержимого 12. Упомянутый ключ (KD), в свою очередь, включается в лицензию 16, соответствующую содержимому 12. Часто такой ключ (KD) зашифровывается в соответствии с открытым ключом, таким как открытый ключ вычислительного устройства 14 (PU-C), на котором должно воспроизводиться содержимое 12, давая в результате (PU-C(KD)). Следует отметить, что могут использоваться другие открытые ключи, такие как, например, открытый ключ пользователя, открытый ключ группы, членом которой является пользователь, и т.д.

Отметим, что в дополнение к ограничению действий, которые пользователь может осуществлять по отношению к распространяемому цифровому содержимому 12, владельцу содержимого или иному подобному лицу может также быть желательным определить (измерить) степень использования такого содержимого 12 данным пользователем, данным вычислительным устройством и т.п. Например, владельцу содержимого может быть желательным знать, сколько раз содержимое 12 было воспроизведено, ввиду того, что пользователю начисляется плата на этой основе, ввиду того, что владелец содержимого получает плату на этой основе, или т.п. Соответственно, владельцу содержимого может быть желательным знать, сколько раз содержимое было скопировано, при условии, что эта опция доступна, сколько раз содержимое 12 было включено в другую часть содержимого, вновь при условии, что данная опция доступна, как долго содержимое воспроизводится, время суток, когда содержимое воспроизводится, и т.д. Короче говоря, владельцу содержимого или иному подобному лицу может также быть желательным определить (измерить) степень использования такого содержимого любым способом, позволяющим действительно измерить или иным образом осуществить отсчет или накопление. Таким образом, доверительный компонент 18 на вычислительном устройстве 14 может быть использован для выполнения такой функции измерения и сохранения полученных при этом измеренных данных в защищенном ЗУ 22.

В общем случае измерение может означать отсчет или накопление иным образом некоторой величины, относящейся к части содержимого 12, причем указанная величина представляет величину, которая должна измеряться в соответствии с потребностями владельца содержимого или иного подобного лица. Как отмечено

выше, измерение в типовом случае может базироваться на количестве раз обращений к содержимому 12 для воспроизведения, копирования, переноса и т.п., величине времени воспроизведения содержимого 12 и т.п. Разумеется, существуют другие формы измерения, и любые другие формы измерения могут быть использованы в связи с настоящим изобретением, как изложено ниже.

Понятно, что измерение полезно по многим причинам, включая обратную связь, финансовые причины и т.п. Например, статистика использования части содержимого 12 может быть важна для владельца содержимого в качестве указателя популярности, полезности, признания, занимательности и т.п. содержимого. В качестве другого примера, статистика использования части содержимого 12 может быть использована для определения вознаграждения автору части содержимого 12, даже если такой автор является одним из многих авторов. В качестве еще одного примера, статистика использования части содержимого 12 может использоваться для вычисления денежной суммы, причитающейся владельцу содержимого. В последнем случае, в частности, понятно, что содержимое 12, такое как музыкальная композиция, может лицензироваться на основе числа использований, на основе единого платежа или на основе комбинации этих подходов. Таким образом, лицензионная плата, формируемая для владельца содержимого при использовании содержимого 12, может изменяться радикальным образом на основе лицензирования и, в частности, на основе того, базируется ли лицензионная плата на фиксированной сумме или на сумме за количество использований.

Кроме того, поскольку детальное измерение еще не выполнялось, вполне вероятно, что обеспечение возможности выполнения такого детального измерения создаст будущие коммерческие модели, недоступные до настоящего времени. Например, стоимость за представление рекламы (содержимое 12), которая в настоящее время базируется главным образом на предварительно установленной и фиксированной ставке, сможет тогда базироваться на том, какое количество воспроизведений рекламы/содержимого 12 было реализовано, как это измерено способом, предусматриваемым настоящим изобретением. В качестве другого примера, телевизионная программа (содержимое 12) тарифицируется в настоящее время на основе, по меньшей мере, доли ее на рынке, как это измерено службой определения рейтинга, то такой рейтинг является просто оценкой, основанной на довольно непредставительной статистической выборке, в то время как в настоящем изобретении такой рейтинг может основываться на детальном измерении количества зрителей/пользователей такой программы/содержимого 12.

Отметим, что хотя доступ и использование содержимого 12 пользователем на вычислительном устройстве 14 могут быть измерены относительно простым способом, не существует никакой архитектуры или способа для (1) определения того, что измеряется, (2) определения того, каким образом данные, полученные в результате измерения, должны храниться на вычислительном устройстве 14, (3) определения службы измерений для сбора измеренных данных с каждого из различных вычислительных устройств или (4) для определения того, каким образом измеренные данные должны сообщаться в службу измерений.

Соответственно, существует потребность в архитектуре и способе, которые обеспечивают измерение данных и сообщение измеренных данных в службу измерений. В частности, существует потребность в архитектуре и способе, которые определяют, что должно измеряться, определяют, каким образом данные, полученные в результате измерения, должны храниться на вычислительном устройстве 14,

определяют службу измерений для сбора измеренных данных с каждого из различных вычислительных устройств и определяют, каким образом измеренные данные должны сообщаться в службу измерений.

Сущность изобретения

Вышеуказанные потребности удовлетворяются, по меньшей мере частично, настоящим изобретением, в котором предусмотрен способ передачи накопленных измеренных данных от клиента в службу измерений. Каждый набор измеренных данных индексируется в базе данных измерений клиента в соответствии с идентификатором измерений (MID) и дополнительно индексируется в базе данных измерений в соответствии с идентификатором, ассоциированным с содержимым (KID).

В этом способе клиент выбирает конкретный идентификатор измерений MID и выбирает, по меньшей мере, часть измеренных данных в базе данных измерений, содержащей выбранный идентификатор MID, где выбранные измеренные данные упорядочены в соответствии с идентификатором KID, ассоциированным с содержимым. Затем клиент формирует запрос на основе выбранных измеренных данных и посылает сформированный запрос в службу измерений. Служба измерений получает измеренные данные из запроса, сохраняет их и формирует ответ, который должен быть возвращен клиенту на основании запроса.

Клиент получает ответ из службы измерений, включая список идентификаторов KID выбранных данных измерений в запросе, и подтверждает, что ответ соответствует заросу. После этого клиент обрабатывает список идентификаторов KID в ответе путем, для каждого идентификатора KID, удаления измеренных данных из базы данных измерений, содержащей выбранные идентификаторы MID и KID.

Краткое описание чертежей

Изложенная выше сущность изобретения, а также последующее детальное описание вариантов осуществления настоящего изобретения могут быть более глубоко поняты при изучении во взаимосвязи с чертежами. В целях иллюстрации изобретения на чертежах показаны варианты осуществления, которые в настоящее время являются предпочтительными. Однако понятно, что изобретение не ограничено именно описанными и показанными конфигурациями и инструментальными средствами. На чертежах представлено следующее:

фиг.1 - блок-схема, иллюстрирующая архитектуру правоприменения на примере основанной на доверительных отношениях системы, включающей в себя клиента, имеющего базу данных измерений, и службу измерений, принимающую от него измеренные данные;

фиг.2 - блок-схема, представляющая универсальную компьютерную систему, в которой могут быть воплощены аспекты настоящего изобретения и/или его части;

фиг.3 - блок-схема, иллюстрирующая соотношение между цифровым содержимым, одной или более цифровых лицензий, связанных с содержимым, и измеренными данными в базе данных измерений по фиг.1, в соответствии с одним вариантом осуществления настоящего изобретения и

фиг.4 - блок-схема, показывающая основные этапы, выполняемые клиентом и службой измерений по фиг.1 при передаче измеренных данных от клиента к службе измерений, в соответствии с одним вариантом осуществления настоящего изобретения.

Детальное описание изобретения

Компьютерная среда

Фиг.1 и последующее изложение предназначены для того, чтобы дать краткое обобщенное описание подходящей вычислительной среды, в которой может быть

реализовано настоящее изобретение и/или его части. Хотя не является обязательным, однако изобретение описано в общем контексте исполняемых компьютером команд, таких как программные модули, исполняемые компьютером, таким как клиентская рабочая станция или сервер. В общем случае программные модули включают в себя стандартные программы, программы, объекты, компоненты, структуры данных и т.д., которые выполняют конкретные задачи или реализуют некоторые абстрактные типы данных. Кроме того, понятно, что изобретение и/или его части могут быть реализованы с использованием других конфигураций вычислительных систем, включая портативные устройства, мультипроцессорные системы, микропроцессорные или программируемые приборы бытовой электроники, сетевые ПК, миникомпьютеры, центральные компьютеры и т.п. Изобретение также может быть реализовано в распределенных вычислительных средах, где задачи выполняются удаленными устройствами обработки, которые связаны коммуникационной сетью. В распределенной вычислительной среде программные модули и другие данные могут размещаться как в локальных, так и удаленных устройствах памяти.

Как показано на фиг.2, приведенная для примера универсальная вычислительная система включает в себя обычный персональный компьютер 120 или тому подобное средство, включающее в себя блок 121 обработки, системную память 122 и системную шину 123, которая связывает различные системные компоненты, включая системную память, с блоком 121 обработки. Системная шина 123 может быть любой из различных типов шинных структур, включая шину памяти или контроллер памяти, шину периферийных устройств и локальную шину, использующую любую из разнообразных шинных архитектур. Системная память включает в себя постоянную память (ПЗУ, ROM) 124 и оперативную память (ОЗУ, RAM) 125. Базовая система ввода/вывода (BIOS) 126, содержащая базовые подпрограммы, которые способствуют переносу информации между элементами в компьютере 120, например, при запуске, в типовом случае сохранена в ПЗУ 124.

Персональный компьютер 120 может дополнительно включать в себя дисковод 127 жесткого диска для считывания с жесткого диска (не показан) и записи на него, дисковод 128 магнитного диска для считывания со съемного магнитного диска 129 или записи на него, дисковод 130 оптического диска для считывания со съемного оптического диска 131, такого как CD-ROM или другой оптический носитель, или записи на него. Дисковод 127 жесткого диска, дисковод 128 магнитного диска, дисковод 130 оптического диска соединены с системной шиной 123 посредством интерфейса 132 дисковода жесткого диска, интерфейса 133 дисковода магнитного диска и интерфейса 134 дисковода оптического диска соответственно. Дисководы и соответствующие им машиночитаемые носители обеспечивают энергонезависимое хранение считываемых компьютером инструкций, структур данных, программных модулей и других данных для персонального компьютера 120.

Хотя описанная примерная среда использует жесткий диск, съемный магнитный диск 129 и съемный оптический диск 131, понятно, что другие типы машиночитаемых носителей, которые могут хранить данные, к которым обращается компьютер, могут также использоваться в примерной операционной среде. Такие другие типы носиелей включают в себя кассеты на магнитных лентах, карты флэш-памяти, цифровые видеодиски (DVD), картриджи Бернулли, ОЗУ, ПЗУ и т.п.

Ряд программных модулей может храниться на жестком диске, магнитном диске 129, оптическом диске 131, ПЗУ 124 и ОЗУ 125, включая операционную систему 135, одну и более прикладных программ (приложений) 136, другие

программные модули 137 и программные данные 138. Пользователь может вводить команды и информацию в персональный компьютер 120 посредством устройств ввода, например, клавиатуры 140 и координатно-указательного устройства 142. Другие устройства ввода (не показаны) могут включать в себя микрофон, джойстик, игровую панель, спутниковую параболическую антенну, сканер и т.п. Эти и другие устройства ввода часто соединяются с блоком 121 обработки через интерфейс 146 последовательного порта, связанный с системной шиной, но они могут быть соединены и посредством других интерфейсов, таких как параллельный порт, игровой порт или универсальная последовательная шина (USB) и т.д. Монитор 147 или иное устройство отображения также соединено с системной шиной 123 через интерфейс, например, такой как видеоадаптер 148. Помимо монитора 147, персональный компьютер в типовом случае включает в себя другие периферийные устройства вывода (не показаны), например громкоговорители и принтеры. Приведенная на фиг.2 примерная система также включает в себя хост-адаптер 155, шину 156 интерфейса малых компьютерных систем (SCSI) и внешнее ЗУ 162, соединенное с шиной SCSI 156.

Персональный компьютер 120 может работать в сетевой среде с использованием логических соединений с одним или более удаленными компьютерами, такими как удаленный компьютер 149. Удаленный компьютер 149 может представлять собой другой персональный компьютер (ПК), сервер, маршрутизатор, сетевой ПК, одноранговое устройство или другой обычный сетевой узел и в типовом случае включает в себя многие или все из элементов, описанных выше применительно к компьютеру 120, хотя на фиг.2 показано только устройство 150 памяти. Логические соединения, показанные на фиг.2, включают в себя локальную сеть (LAN) 151 и глобальную сеть (сеть широкого охвата - WAN) 152. Такие сетевые среды являются общеизвестными в офисах, компьютерных сетях предприятий, интранетах и в Интернет.

При использовании в сетевой среде локальной сети (LAN) персональный компьютер 120 соединяется с локальной сетью 151 через сетевой интерфейс или адаптер 153. При использовании в сетевой среде глобальной сети (WAN) персональный компьютер 120 в типовом случае включает в себя модем 154 или иное средство для установления связи в глобальной сети 152, такой как Интернет. Модем 154, который может быть внутренним или внешним, соединен с системной шиной 123 через интерфейс 146 последовательного порта. В сетевой среде программные модули, изображенные по отношению к персональному компьютеру 120, или их части могут быть сохранены в удаленном устройстве памяти. Следует иметь в виду, что показанные сетевые соединения приведены для примера, и что могут быть использованы и другие средства установления канала связи между компьютерами.

Определение степени доступа к содержимому 12

В настоящем изобретении доступ к содержимому 12 на вычислительном устройстве 14 в соответствии с системой 10 защиты содержимого измеряется в соответствии с определением того, что должно измеряться, и данные, полученные в процессе измерений, сохраняются на вычислительном устройстве 14 или еще где-либо. Такие измеренные данные с каждого из различных вычислительных устройств 14 периодически передаются в службу 24 измерений (фиг.1), которая собирает измеренные данные от каждого из различных вычислительных устройств 14, в частности, переданные службе 24 измерений в соответствии с установленной

процедурой.

Заметим, что термином «защита содержимого» обозначается целый спектр методов и технологий для защиты цифрового содержимого 12 так, чтобы такое содержимое 12 не могло быть использовано способом, несовместимым с желанием владельца и/или провайдера содержимого. Методы включают, в том числе, защиту от копирования (CP), защиту канала (LP), условный доступ (CA), управление правами (RM) и цифровое управление правами (DRM). Основой любой системы 10 защиты содержимого является то, что только доверительное приложение, которое гарантирует надлежащее соблюдение прямо и/или косвенно выраженных правил использования защищенного содержимого, может получать доступ к нему в незащищенной форме. В типовом случае содержимое 12 защищено путем шифрования некоторым способом, причем только доверительные стороны имеют возможность дешифровать его.

Защита от копирования в самом строгом смысле специально применяется к содержимому 12, хранящемуся в устройстве, в то время как защита канала применяется к содержимому 12, передаваемому между приложениями/устройствами по среде передачи. Условный доступ можно представить как более сложную форму защиты канала, при которой платные программы, каналы и/или фильмы передаются в зашифрованном виде. Только абонентам, которые оплатили доступ к такому содержимому 12, предоставляются ключи, необходимые для его дешифрования.

Цифровое управление правами представляет собой расширяемую архитектуру, где правила, касающиеся санкционированного использования конкретной части содержимого 12, являются явно выраженными и связаны или ассоциированы с самим содержимым. Механизмы DRM могут поддерживать более обогащенные и более содержательные правила, чем в случае других методов, при обеспечении большей степени управления и гибкости на уровне отдельных частей содержимого или даже подкомпонентов такого содержимого. Пример системы цифрового управления правами описан в патентной заявке США № 09/290,363 от 12 апреля 1999 и в предварительной заявке США № 60/126,614 от 27 марта 1999, которые включены во всей своей полноте в настоящее описание посредством ссылки.

Управление правами является формой DRM, которая организационно основана на том, что содержимое 12 может быть защищено для обеспечения доступа только в рамках некоторой организации или ее подразделения. Пример системы управления правами описан в патентных заявках США № 10/185,527; 10/185,278 и 10/185,511, каждая из которых подана 28 июня 2002 и включена во всей своей полноте в настоящее описание посредством ссылки.

Определение того, что должно измеряться

В одном варианте осуществления настоящего изобретения измерение на вычислительном устройстве выполняется под контролем и при содействии доверительного компонента 18 на вычислительном устройстве 14 в ходе использования лицензии 16 на воспроизведение соответствующего содержимого 12. В таком варианте осуществления использование содержимого 12 и доступ к нему и воспроизведение содержимого 12 измеряется, если лицензия 16 включает в себя тег измерения, такой как может использоваться в основанной на XML (расширяемый язык разметки) лицензии 16 или тому подобном. Таким образом, понятно, что измерение выполняется по отношению к содержимому 12, даже если решение относительно того, следует ли осуществлять измерение, базируется на наличии тега измерения в лицензии 16.

Например, следующая часть лицензии 16 включает в себя тег идентификатора измерения (MID), и поэтому соответствующее содержимое 12 измеряется доверительным компонентом 18 в ходе воспроизведения такого содержимого 12:

```
<LICENSE version="2.0.0.0">
    ...
    <LICENSORINFO>
        <DATA>
            ...
            <KID>FgA3Mep5+UiW5yB2CuevGg==</KID>
            <MID>UiW5yBMep2CuevGg5+FgA3==</MID>
            ...
        </DATA>
        ...
    </LICENSORINFO>
    ...
</LICENSE>
```

Заметим, что данные, ассоциированные с тегом MID (далее «MID»), могут представлять собой 16-байтовую идентификацию, кодированную по основанию 64. В одном варианте осуществления настоящего изобретения такой идентификатор MID идентифицирует получателя измеренных данных, собранных в связи с такой лицензией 16, как изложено более детально ниже. Также отметим, что тег KID идентифицирует содержимое 12, с которым связана лицензия 16, и, по меньшей мере, в некоторых случаях данные, ассоциированные с таким тегом KID (далее «KID»), могут представлять значение, из которого может быть выведен ключ содержимого (KD) для дешифрования содержимого 12.

Доверительный компонент 18 может собирать измеренные данные любого конкретного типа в связи с использованием содержимого 12 без отклонения от сущности и объема настоящего изобретения. В одном варианте осуществления настоящего изобретения доверительный компонент 18 поддерживает отсчет в защищенном ЗУ 22 для каждого права воспроизведения (PLAY (воспроизведение), COPY (копирование), TRANSFER (перенос), EDIT (редактирование) и т.д.) и сообщает приращение каждому такому отсчету, когда право использовано для доступа к содержимому 12. Отметим, что защищенное ЗУ 22 используется для хранения измеренных данных для воспрепятствования злоупотреблениям со стороны пользователя или посторонних лиц по отношению к таким измеренным данным. В противном случае недобросовестный пользователь, которому, например, производится начисление платы за каждое использование, мог бы изменить измеренные данные таким образом, чтобы представить уменьшенное количество использований, чем имело место на самом деле.

В альтернативном варианте осуществления настоящего изобретения тег MID может включать в себя данные, по которым отсчитываются права использования (не показано), и/или данные по другим аспектам использования содержимого 12, которые должны измеряться, и то, каким образом должны осуществляться измерения (также не показано). Таким образом, как было указано, доверительный компонент 18 может выполнять такое измерение, как количество времени воспроизведения содержимого 12, количество раз воспроизведения содержимого 12, количество раз запуска воспроизведения, количество раз остановки воспроизведения содержимого, число нажатий клавиш или движений мыши в процессе воспроизведения и т.д., и сохранять соответствующие измеренные данные в защищенном ЗУ 22.

Сохранение данных, полученных при измерениях

Понятно, что доверительный компонент 18, накапливает измеренные данные по отношению к части содержимого 12 в связи с использованием соответствующей лицензии 16 для воспроизведения такого содержимого 12 (т.е. доступа к нему) и соответственно сохраняет такие накопленные данные измерений в защищенном ЗУ 22, как показано на фиг.3. Также понятно, что дополнительно доверительный компонент 18 может накапливать данные лицензии по отношению к использованию лицензии 16 для воспроизведения и может также соответствующим образом сохранять такие накопленные данные лицензии в защищенном ЗУ 22 (не показано).

В одном варианте осуществления настоящего изобретения, как показано на фиг.3, доверительный компонент 18 сохраняет измеренные данные в защищенном ЗУ в базе 26 данных измерений в соответствии с идентификатором MID в лицензии 16, который инициировал измерение, результатом которого явились измеренные данные, а также в соответствии с идентификатором KID соответствующего содержимого 12, для которого проводятся измерения, также указанным в такой лицензии 16. В частности, доверительный компонент 18 сохраняет измеренные данные в защищенном ЗУ 22 в базе 26 данных измерений в соответствии с упомянутым идентификатором MID в качестве значения первичного индекса, а также в соответствии с упомянутым идентификатором KID в качестве значения вторичного индекса. Таким образом, для любого конкретного использования лицензии 16, имеющей конкретные идентификаторы MID и KID, чтобы воспроизвести часть содержимого 12, имеющего конкретный идентификатор KID, доверительный компонент 18 обновляет соответствующее значение индекса идентификатора MID, KID в базе 26 данных в защищенном ЗУ для отражения этого использования. Например, если это содержимое дважды воспроизводилось (PLAY) и один раз копировалось (COPY), то доверительный компонент 18 может придать дважды приращение значению счета PLAY и придать однократно приращение значению счета COPY для соответствующего значения индекса MID, KID в базе 26 данных в защищенном ЗУ 22.

Отметим, что каждая из множества лицензий 16 может разрешить воспроизведение одной и той же части содержимого 12, но может иметь тот же самый или отличающийся идентификатор MID. Таким образом, если каждая такая лицензия 16 имеет тот же самый идентификатор MID и используется однократно для воспроизведения части содержимого 12, счет воспроизведений для значения индекса MID, KID получает приращение дважды для двух случаев воспроизведений. Соответственно, если каждая из таких двух лицензий 16 имеет отличающийся идентификатор MID (MID1 и MID2) и используется однократно для воспроизведения части содержимого 12, то счет воспроизведений для значения индекса MID1, KID получает приращение однократно для одного воспроизведения (PLAY) и счет воспроизведений для значения индекса MID2, KID аналогичным образом получает приращение однократно для одного воспроизведения (PLAY).

Служба измерений

Измеренные данные, собранные доверительным компонентом 18 в базе 26 данных измерений в защищенном ЗУ 22, периодически пересылаются в централизованную службу 24 измерений, причем служба 24 измерений может принимать измеренные данные от множества вычислительных устройств и обрабатывать их надлежащим образом. Такая обработка может представлять собой любую подходящую обработку без отклонения от сущности и объема настоящего изобретения. Например, если автор части содержимого 12 должен собирать роялти на основе за каждое использование,

служба измерений может агрегировать все отсчеты использования за определенный период времени по отношению к конкретной части содержимого 12 и сообщать об этом автору и/или организации, выплачивающей роялти. Альтернативно, служба измерений может просто получать и сохранять измеренные данные для извлечения их другой службой, которая выполняет обработку, или может периодически направлять сохраненные измеренные данные другой службе.

Независимо от того, какая служба в действительности обрабатывает измеренные данные, понятно, что поскольку каждая часть измеренных данных сохраняется в базе 26 данных измерений согласно ее значению индекса MID, KID, такая часть данных может пересылаться к службе 24 измерений с указанным значением индекса MID, KID, а также обрабатываться в соответствии с указанным значением индекса MID, KID. Соответственно, обработка отправленных измеренных данных может также выполняться в соответствии с этим значением индекса MID, KID. Таким образом, в качестве примера, если владелец части содержимого 12 должен собирать твердое комиссионное вознаграждение, если суммарное значение всех использований частей содержимого 12 достигает некоторого значения, то такое агрегирование может выполняться на основе значения индекса KID, связанного с измеренными данными, соответствующими такой части содержимого 12, посредством службы 24 измерений.

В одном варианте осуществления настоящего изобретения множество служб 28 измерений может быть реализовано для приема переданных измеренных данных, и каждая часть измеренных данных направляется в конкретную службу 24 измерений на основе идентификатора MID, ассоциированного с конкретной частью измеренных данных. Понятно, что служба 24 измерений может быть ассоциирована с одним или более идентификаторами MID, и, таким образом, может принимать измеренные данные с такими одним или более идентификаторами MID.

Ассоциирование идентификатора MID со службой 24 измерений может устанавливаться органом управления содержанием, выпускающим сертификат 30 измерений, включающий в себя идентификатор MID, идентификацию соответствующей службы 24 измерений, такую как URL (универсальный указатель ресурсов), открытый ключ (PU-M) и цифровую подпись (сигнатуру). Таким образом, доверительный компонент 18 на каждом вычислительном устройстве 14, который должен сообщать измеренные данные, имеющие конкретный идентификатор MID, ассоциированный с ними, соответствующей службе 24 измерений, должен иметь соответствующий сертификат 30 измерений, хотя бы для идентификации конкретного идентификатора MID в службе 24 измерений. В типовом случае доверительный компонент 18 может быть снабжен одним или более сертификатов 30 измерений при инициализации и/или в процессе регулярных обновлений данных.

Передача измеренных данных в службу измерений

Вычислительное устройство 14 (далее «клиент 14») накапливает измеренные данные в своей базе 26 данных измерений в течение заданного времени и, таким образом, может периодически посылать эти измеренные данные в одну или более служб 28 измерений. Периодичность передачи может соответствовать любому подходящему периоду без отклонения от сущности и объема настоящего изобретения. Например, такая периодичность может соответствовать ежедневной, еженедельной, двухнедельной, ежемесячной передаче и т.п. Альтернативно, такая периодичность может основываться на том, что база 26 данных измерений достигает некоторого объема данных или накапливает определенное количество измеренных данных.

При передаче измеренных данных клиент 14 может передать все измеренные

данные, накопленные в его базе 26 данных измерений, или может передать только часть измеренных данных, накопленных в его базе 26 данных измерений. В частности, в одном варианте осуществления настоящего изобретения клиент 14 передает измеренные данные, накопленные в его базе 26 данных измерений, на основе сертификата 30 измерений. Таким образом, если клиент 14 не имеет сертификата 30 измерений, соответствующего определенным измеренным данным в базе 26 данных измерений, такие определенные измеренные данные не передаются.

Во всяком случае, со ссылкой на фиг.4, в одном варианте осуществления настоящего изобретения клиент 14 передает измеренные данные, накопленные в его базе 26 данных измерений, на основе сертификата 30 измерений в соответствии со следующей процедурой. Предварительно клиент 14 выбирает конкретный сертификат 30 измерений и проверяет его действительность на основе его цифровой подписи (этап 401) и затем определяет из проверенного действительного сертификата 30 измерений идентификатор MID, указанный в нем (этап 403). Затем на основе такого идентификатора MID клиент 14 выбирает и копирует в предварительно определенный формат, по меньшей мере, часть измеренных данных в базе 26 данных измерений, имеющих такой идентификатор MID, ассоциированный с ними (этап 405).

Отметим, что поскольку все измеренные данные в базе данных измерений индексированы в первую очередь на основе ассоциированного с ними идентификатора MID, измеренные данные, имеющие конкретный ассоциированный с ними идентификатор MID, должны быть расположены вместе, по меньшей мере, в логическом смысле, и поэтому выбор измеренных данных, имеющих конкретный ассоциированный с ними идентификатор MID, должен быть относительно простой задачей. Также отметим, что поскольку все измеренные данные в базе данных измерений индексированы во вторую очередь на основе ассоциированного с ними идентификатора KID, выбранные измеренные данные должны быть уже организованы в соответствии с ассоциированным с ними идентификатором KID. Таким образом, выбранные измеренные данные должны быть списком отсчетов или тому подобной структурой, организованной в соответствии с идентификатором KID, и могут, например, быть упорядочены в формате XML следующим образом:

```
<KID0>
        <COUNT1>a</COUNT1>
        <COUNT2>b</COUNT2>
        <COUNT3>c</COUNT3>
</KID0>
<KID1>
        <COUNT4>d</COUNT4>
        <COUNT5>e</COUNT5>
</KID1>
<KID2>
        <COUNT6>f</COUNT6>
</KID2>
```

Заметим, что измеренные данные могут уже быть в формате XML в базе 26 данных измерений клиента 14, и в этом случае такие измеренные данные могут дословно копироваться в запрос.

В одном варианте осуществления настоящего изобретения клиент 14 с использованием сформатированных выбранных измеренных данных формирует запрос на основе сформатированных измеренных данных и сертификата 30 измерений (этап 407). Такой запрос может включать в себя, например,

идентификатор MID из сертификата 30 измерений, идентификацию в форме указателя URL или другую идентификацию соответствующей службы 24 измерений из сертификата 30 измерений, ИД транзакции (TID), выбранный для запроса, и сформатированные измеренные данные. Заметим, что для защиты сформатированных измеренных данных от просмотра другими сторонами, указанные сформатированные измеренные данные в запросе должны зашифровываться в соответствии с симметричным ключом доступа для получения структуры типа (ключ доступа(измеренные данные)), и ключ доступа сам должен быть введен в запрос в зашифрованном виде в соответствии с ключом (PU-M) из сертификата 30 измерений для получения в результате зашифрованной структуры (PU-M (ключ доступа)). Такой ключ доступа может представлять собой любой подходящий ключ без отклонения от сущности и объема настоящего изобретения. Например, ключ доступа может быть получен клиентом 14 частично из идентификатора MID по односторонней процедуре с возможностью воспроизведения ключа.

Заметим, что идентификатор TID может представлять собой 16-байтовые идентификационные данные, кодированные по основанию 64, и генерируется случайным образом каждый раз, когда запрос успешно передан, и на него получен ответ, и соответствующие измеренные данные удалены из базы 26 данных измерений, как описано более подробно ниже. Как детально описано ниже, клиент 14 уже сформировал идентификатор TID настоящего запроса для идентификатора MID после успешного завершения предыдущего запроса, соответствующего идентификатору MID, и сохранил указанный сформированный идентификатор TID в базе 26 данных измерений в соответствии с идентификатором MID настоящего запроса для извлечения и использования в связи с настоящим запросом для идентификатора MID.

При определенных обстоятельствах клиент 14 не сможет сформировать запрос, содержащий все сформатированные измеренные данные. Например, если клиент 14 представляет собой относительно простое устройство с ограниченной памятью, размер запроса может быть ограничен доступным объемом буфера в клиенте 14. Если клиент 14 реально не может сформировать запрос, который должен содержать все сформатированные измеренные данные, то запрос может включать в себя флаг частичных данных. Как описано более подробно ниже, служба 24 измерений, которая предназначена для приема запроса, может иметь, или не иметь никакого касательства к тому, содержит ли принятый запрос все сформатированные измеренные данные, но служба 24 измерений в ответе на запрос будет включать установленный флаг частичных данных, чтобы напомнить клиенту 14 о необходимости посылки следующего запроса с дополнительными сформатированными измеренными данными.

Как указано выше, сформатированные измеренные данные в запросе включают в себя сформатированные измеренные данные, зашифрованные ключом доступа для воспрепятствования их просмотру другими сторонами. Аналогичным образом, запрос или, по меньшей мере, его часть должны хешироваться в соответствии с ключом доступа для получения значения хеш-функции и значение хеш-функции должно включаться в запрос для обнаружения модифицирования, осуществленного другими сторонами. Понятно, что если запрос или, по меньшей мере, его часть модифицированы после вычисления значения хеш-функции как преднамеренно, так и ненамеренным образом значение хеш-функции не пройдет проверку.

Пример сформированного запроса со сформатированными измеренными данными, как описано выше, имеет следующий вид:

```
<METERDATA type="challenge">
    <DATA>
        <MID>UiW5yBMep2CuevGg5+FgA3==</MID>
        <TID>Mep2CuevGgUiW5yB5+FgA3==</TID>
        <PASSWORD>encrypted, base64 password</PASSWORD>
        <RECORDS>
            <KID value="KID1">
                <ACTION value="Play">5</ACTION>
            </KID>
            <KID value="KID2">
                <ACTION value="Play">71</ACTION>
                <ACTION value="Burn">2</ACTION>
            </KID>
            ...
        </RECORDS>
        <PARTIALDATA>set</PARTIALDATA>
    </DATA>
    <HASH>
        <HASHALGORITHM type="HMAC" />
        <VALUE>
            Base64-encoded hash
        </VALUE>
    </HASH>
</METERDATA>
```

Отметим, что запрос идентифицируется как таковой путем включения с тегом METERDATA (измеренные данные) типа атрибута, установленного как «запрос».

Запрос, сформированный клиентом 14, посылается в службу 24 измерений посредством соответствующего соединения между ними, например сетевого соединения (этап 409). Такое соединение может представлять собой любое соединение без отклонения от сущности и объема изобретения. Например, в одном сценарии соединение может обеспечивать то, что клиент/вычислительное устройство 14 непосредственно связывается со службой 24 измерений посредством взаимно приемлемого протокола, такого как HTTP, по сети, такой как Интернет. В другом сценарии, где клиент 14 и служба 24 измерений непосредственно связаны, соединение может соответствовать технологии прямого соединения, например, соединения посредством шины USB-1394.

После осуществления приема служба 24 измерений применяет ключ (PR-M) к структуре (PU-M(ключ доступа)) из принятого запроса для получения ключа доступа (этап 411) и проверяет значение хеш-функции из принятого запроса на основе полученного ключа доступа (этап 413). Если по некоторой причине значение хеш-функции не проходит проверку, служба 24 измерений может запросить клиента направить еще один запрос для того же идентификатора MID или может просто игнорировать запрос, в последнем случае клиент 14 продолжает накапливать измеренные данные для данного идентификатора MID до истечения следующего периода для передачи сообщения, и в этот момент клиент 14 посылает запрос, чтобы в действительности сообщить измеренные данные для идентификатора MID из двух предыдущих периодов передач.

При условии, что значение хеш-функции подтверждено, служба 24 измерений может затем применить ключ доступа к структуре (ключ доступа (измеренные данные)) из

принятого запроса для получения измеренных данных (этап 415) и затем сохраняет полученные измеренные данные соответствующим способом (этап 417). Заметим, что сохранение полученных измеренных данных может быть выполнено любым подходящим способом без отклонения от сущности и объема настоящего изобретения. Конкретное местоположение и способ хранения релевантны, главным образом, для другой службы 32 (фиг.1), которая извлекает и использует такие сохраненные измеренные данные.

Для завершения транзакции служба измерений формирует ответ, который должен быть возвращен клиенту 14 на основе запроса (этап 419). На основе такого ответа, как можно видеть, клиент 14 удаляет выбранные измеренные данные, которые являются основой запроса, из базы 26 данных измерений данного клиента 14.

В любом случае, и в одном варианте осуществления настоящего изобретения, содержимое сформированного ответа подобно содержимому соответствующего запроса, и в действительности может содержать части запроса, скопированного в него. Таким образом, ответ может, например, включать в себя идентификаторы MID и TID из запроса и, по меньшей мере, часть сформатированных измеренных данных. Заметим, в отношении последнего вопроса, что службе 24 измерений посредством ответа необходимо только информировать клиента 14, что измеренные данные, имеющие определенные идентификаторы KID, были обработаны, и не требуется включать текущие обработанные измеренные данные. Соответственно, часть сформатированных измеренных данных, которые должны быть включены в ответ, представляет собой список идентификаторов KID обработанных измеренных данных.

Как и ранее, для защиты списка идентификаторов KID в ответе от просмотра другими сторонами, такой список может быть зашифрован в соответствии с ключом доступа, полученным из запроса, или другим ключом, хотя понятно, что такой список может не требовать шифрования, если он не считается конфиденциальным по своему характеру. Если ключ доступа из запроса использован, такой ключ доступа не требуется включать в ответ в зашифрованной форме, если клиент 14 может вывести его из идентификатора MID или некоторого другого источника.

Как отмечено выше, если клиент 14 не может сформировать запрос, который будет включать в себя все сформатированные измеренные данные, то запрос включает в себя установленный флаг частичных данных. В таком случае служба 24 измерений, принимающая запрос и отвечающая на него, включает в ответ установленный флаг частичных данных, чтобы напомнить клиенту 14 о необходимости передачи другого запроса с дополнительными сформатированными измеренными данными. Наконец, ответ или, по меньшей мере, его часть должны хешироваться в соответствии с ключом доступа для получения значения хеш-функции, и значение хеш-функции должно включаться в ответ для обнаружения возможных модификаций, осуществленных другими сторонами. Понятно, что если ответ или, по меньшей мере, его часть модифицированы после получения значения хеш-функции преднамеренно или ненамеренным образом, то значение хеш-функции не пройдет проверку.

Пример сформированного запроса имеет следующий вид:

```
<METERDATA type="response">
    <DATA>
        <MID>UiW5yBMep2CuevGg5+FgA3==</MID>
        <TID>Mep2CuevGgUiW5yB5+FgA3==</TID>
        <COMMAND>RESET</COMMAND>
        <RECORDS>
            <KID value="KID1" />
            <KID value="KID2" />
            ...
        </RECORDS>
        <PARTIALDATA>set</PARTIALDATA>
    </DATA>
    <HASH>
        <HASHALGORITHM type="HMAC" />
        <VALUE>
            Base64-encoded hash
        </VALUE>
    </HASH>
</METERDATA>
```

Отметим, что ответ идентифицируется как таковой путем включения с тегом METERDATA (измеренные данные) типа атрибута, установленного как «ответ». Заметим также, что ответ включает в себя команду RESET (сброс), которая, как показано ниже, является по существу разрешением для клиента 14 удалить выбранные измеренные данные из его базы 26 данных измерений.

Ответ, сформированный службой 24 измерений, посылается клиенту 14 посредством соответствующего соединения между ними, например сетевого соединения (этап 421). После приема клиент 14 получает ключ доступа, либо путем повторного его вывода, либо путем извлечения сохраненной его копии, и проверяет значение хеш-функции из принятого ответа на основе полученного ключа доступа (этап 423). Если по некоторой причине значение хеш-функции не проходит проверку, то клиент 14 может запросить от службы 24 измерений получение другого ответа на тот же самый запрос, или может просто проигнорировать ответ, в последнем случае клиент 14 продолжает накапливать измеренные данные для идентификатора MID до истечения следующего периода передачи сообщения, и в этот момент клиент 14 посылает запрос, чтобы в действительности сообщить измеренные данные для идентификатора MID из двух предыдущих периодов передач.

При условии, что значение хеш-функции прошло проверку, клиент 14 затем подтверждает, что идентификаторы TID и MID в ответе согласуются с идентификатором TID, сохраненным в базе 26 данных измерений с тем же самым идентификатором MID (этап 425). Клиент 14 затем, при необходимости, применяет ключ доступа к зашифрованному списку идентификаторов KID из принятого ответа для получения такого списка и обрабатывает список идентификаторов KID для каждого идентификатора KID в списке, удаляя измеренные данные из базы 26 данных измерений, имеющих значение индекса MID, KID (этап 427). Таким образом, после того как измеренные данные успешно переданы, такие измеренные данные очищаются из базы 26 данных измерений, так что новые измеренные данные могут накапливаться в течение следующего периода передачи.

Заметим, что удаление измеренных данных может выполняться любым подходящим способом без отклонения от сущности и объема настоящего изобретения.

Например, значение индекса MID, KID и все данные, ассоциированные с ним, могут быть удалены, или значение индекса MID, KID может быть оставлено, а удаляются только данные, ассоциированные с ним.

После успешной обработки всех идентификаторов KID в списке ответа, и как упомянуто выше, клиент 14 генерирует идентификатор TID следующего запроса для идентификатора MID и сохраняет сформированный идентификатор TID в базе 26 данных измерений в соответствии с идентификатором MID настоящего запроса для извлечения и использования его в связи со следующим запросом для идентификатора MID (этап 429). Понятно, что такое предварительное генерирование идентификатора TID требует первоначального генерирования идентификатора TID для каждого идентификатора MID, когда такой идентификатор MID впервые вводится в базу 26 данных измерений.

Как можно видеть, использование идентификатора TID в запросе и полученный в результате ответ гарантируют, что накопленные измеренные данные, как сообщено клиентом 14, не отсчитываются многократно службой 24 измерений. В частности, если по какой-либо причине первый запрос с измеренными данными из первого периода передачи принят и сохранен службой 24 измерений, но клиент 14 не смог получить ответ, то этот клиент не будет генерировать новый идентификатор TID для идентификатора MID запроса, а также не будет удалять измеренные данные первого периода передачи сообщения. В таком случае результатом отсутствия генерации нового идентификатора TID является то, что следующий запрос для идентификатора MID с измеренными данными из первого периода передачи и следующего периода передачи будет принят и сохранен службой 24 измерений с последующей реакцией на него этой службой. Однако поскольку следующий запрос будет иметь тот же самый идентификатор TID, что и первый запрос, служба 24 измерений не должна сохранять измеренные данные как из первого периода передачи, так и из следующего периода передачи, как было установлено в следующем запросе, вместе с измеренными данными из первого периода передачи, как было установлено в первом запросе, таким образом, чтобы измеренные данные из первого периода передачи дублировались. Понятно, что это привело бы к двукратному отсчету измеренных данных из первого периода передачи. Вместо этого, служба 24 измерений должна перезаписать измеренные данные из первого периода передачи, как было установлено в первом запросе, измеренными данными из первого периода передачи и следующего периода передачи, как было установлено в следующем запросе. В результате измеренные данные из первого периода передачи в действительности не отсчитываются дважды. Разумеется, для того чтобы служба 24 измерений распознала, что следующий запрос имеет тот же самый идентификатор TID, что и первый запрос, служба 24 измерений должна поддерживать базу данных идентификаторов TID и ассоциированных измеренных данных.

Наконец, после генерации нового идентификатора TID для идентификатора MID запроса, клиент 14 определяет, содержит ли запрос установленный флаг частичных данных (этап 431). Если содержит, то клиент 14 имеет дополнительные измеренные данные для передачи в службу 24 измерений по отношению к данному идентификатору MID запроса и, следовательно, продолжает формировать и посылать один или более дополнительных запросов для сообщения о дополнительных измеренных данных, как на этапах 405-431. Заметим, что такие дополнительные запросы посылаются своевременно, по существу немедленно, не ожидая истечения следующего периода для передачи.

Отметим, что до сих пор не предполагалось, что клиент 14 идентифицируется по отношению к службе 24 измерений. В действительности, может быть целесообразным и даже необходимым скрыть идентификацию клиента 14 от службы измерений, например, ввиду соображений конфиденциальности. Однако, если клиент 14 передает измеренные данные в службу 24 измерений, по меньшей мере, частично, поскольку пользователь клиента 14 согласовал, например, плату на основе измеренного использования, то клиент 14 должен в действительности быть идентифицирован для службы измерений, хотя бы для обеспечения того, что его пользователю будет надлежащим образом осуществляться начисление платы за такое измеренное использование. В типовом случае такая идентификация реализуется путем включения в запрос цифрового сертификата, идентифицирующего клиента 14, пользователя или т.п., при этом цифровой сертификат включает в себя открытый ключ (PU-U) и цифровую подпись, где цифровая подпись, разумеется, может проверяться на ее достоверность. Таким образом, вместо включения хеш-функции в запрос на основе ключа доступа, запрос может содержать цифровую подпись, основанную на ключе (PR-U) и проверяемую на основе ключа (PU-U) из включенного в его состав цифрового сертификата. Аналогичным способом, возможен вариант, когда вместо включения в запрос хеш-функции на основе ключа доступа, ответ может содержать цифровую подпись на основе секретного ключа (PR-M), ассоциированную с сертификатом 30 измерений и проверяемую на основе соответствующего ключа (PU-M) из такого сертификата 30 измерений.

Вывод

Настоящее изобретение может быть реализовано по отношению к любому соответствующему клиенту 14 и службе 24 измерений в предположении, что такой клиент 14 и служба 24 измерений назначают соответствующие доверительные компоненты 18 на них. Понятно, что согласно настоящему изобретению, как описано выше, доступ и другое использование содержимого 12 на клиенте может быть измерено, и измеренные данные могут быть соответствующим образом переданы в службу 24 измерений для соответствующей цели, так что измеренные данные могут быть использованы службой 24 измерений или иной службой 32.

Программирование, необходимое для осуществления процессов, выполняемых в соответствии с настоящим изобретением, является относительно простым и должно быть очевидным для специалистов в области программирования. Поэтому такое программирование здесь не рассматривается. Поэтому любое конкретное программирование может быть использовано для осуществления настоящего изобретения без отклонения от сущности и объема настоящего изобретения.

В изложенном выше описании показано, что настоящее изобретение содержит новую и полезную архитектуру и способ, который реализует измеренные данные и передачу измеренных данных от клиента 14 в службу 24 измерений. Эти архитектура и способ определяют то, что должно измеряться, каким образом данные, полученные в результате измерений, должны сохраняться в вычислительном устройстве 14, а также определяют службу 24 измерений для сбора измеренных данных от каждого из различных вычислительных устройств 14, и каким образом измеренные данные должны передаваться в службу 24 измерений.

Понятно, что в вариантах осуществления, описанных выше, могут производиться изменения без отклонения от принципов изобретения. Поэтому в целом должно быть понятно, что данное изобретение не ограничено конкретными раскрытыми вариантами осуществления, а охватывает видоизменения в пределах сущности объема

настоящего изобретения, как определено в формуле изобретения.

Формула изобретения

1. Способ передачи накопленных измеренных данных от клиента в службу измерений, согласно которому каждый набор измеренных данных индексируется в базе данных измерений клиента в соответствии с идентификатором измерений (MID) и дополнительно индексируется в базе данных измерений в соответствии с идентификатором, ассоциированным с содержимым (KID), при этом клиент выбирает конкретный идентификатор MID, выбирает, по меньшей мере, часть измеренных данных в базе данных измерений, содержащих выбранный идентификатор MID, где выбранные измеренные данные упорядочены в соответствии с идентификатором KID, формирует запрос на основе выбранных измеренных данных, посылает сформированный запрос в службу измерений, при этом служба измерений получает измеренные данные из запроса, сохраняет их и формирует ответ, который должен быть возвращен клиенту на основании запроса, клиент получает ответ из службы измерений, включающий в себя список идентификаторов KID выбранных данных измерений в запросе, подтверждает, что ответ соответствует запросу, и обрабатывает список идентификаторов KID в ответе путем удаления для каждого идентификатора KID измеренных данных из базы данных измерений, содержащих выбранные идентификаторы MID и KID.

2. Способ по п.1, включающий формирование запроса, содержащего идентификатор MID, идентификацию местонахождения службы измерений, идентификатор транзакции (TID), выбранный для запроса, и выбранные измеренные данные.

3. Способ по п.2, включающий формирование запроса, содержащего выбранные измеренные данные, зашифрованные в соответствии с симметричным ключом доступа для получения структуры в форме (ключ доступа (данные измерений)), и дополнительно включающего в себя ключ доступа, зашифрованный в соответствии с открытым ключом (PU-M) службы измерений для получения структуры в форме (PU-M(ключ доступа)), причем служба измерений может применить секретный ключ (PR-M), соответствующий ключу (PU-M) к структуре (PU-M(ключ доступа)) из запроса для получения ключа доступа, может применить полученный ключ доступа к структуре (ключ доступа(данные измерений)) из запроса для получения измеренных данных и может затем сохранить полученные измеренные данные.

4. Способ по п.3, включающий формирование запроса, дополнительно содержащего значение хеш-функции, полученное из хеш-функции, по меньшей мере, части запроса на основе ключа доступа, при этом если, по меньшей мере, часть запроса после этого модифицируется, то значение хеш-функции не проходит проверку, причем служба измерений может проверить значение хеш-функции из запроса на основе ключа доступа.

5. Способ по п.2, включающий формирование запроса, дополнительно содержащего установленный флаг частичных данных, если клиент не может сформировать запрос, который содержит все накопленные измеренные данные в базе данных измерений для выбранного идентификатора MID.

6. Способ по п.1, включающий прием ответа, содержащего идентификатор MID, как было установлено в запросе, идентификатор транзакции (TID), как было установлено в запросе, и, по меньшей мере, часть выбранных измеренных данных, как было установлено в запросе.

7. Способ по п.6, включающий прием ответа, содержащего список идентификаторов KID, по меньшей мере, части выбранных измеренных данных.

8. Способ по п.6, включающий прием ответа, содержащего, по меньшей мере, часть выбранных измеренных данных, зашифрованных в соответствии с симметричным ключом доступа для получения структуры в форме (люч доступа(данные измерений)), и дополнительно включающий в себя получение клиентом ключа доступа и применения полученного ключа доступа к структуре (ключ доступа(данные измерений)) из ответа для получения, по меньшей мере, части измеренных данных.

9. Способ по п.8, включающий прием ответа, дополнительно содержащего значение хеш-функции, полученное из хеш-функции, по меньшей мере, части ответа на основе ключа доступа, и дополнительно включающий в себя проверку клиентом значения хеш-функции из ответа на основе ключа доступа.

10. Способ по п.6, включающий прием ответа, дополнительно содержащего установленный флаг частичных данных, если запрос содержал установленный флаг частичных данных, указывающий на то, что клиент не мог сформировать запрос, который содержит все накопленные измеренные данные в базе данных измерений для выбранного идентификатора MID, и что клиент, таким образом, имеет дополнительные измеренные данные для передачи в службу измерений по отношению к выбранному идентификатору MID запроса.

11. Способ по п.10, дополнительно включающий, если ответ содержит установленный флаг частичных данных, выбор, по меньшей мере, части дополнительных измеренных данных в базе данных измерений, имеющих выбранный идентификатор MID, формирование дополнительного запроса на основе выбранных дополнительных измеренных данных, и передачу сформированного дополнительного запроса в службу измерений.

12. Способ по п.6, в котором подтверждение, что ответ соответствует запросу, включает в себя подтверждение, что идентификатор TID и идентификатор MID в ответе согласуются с идентификатором TID, сохраненным в базе данных измерений с выбранным идентификатором MID.

13. Способ по п.1, дополнительно включающий извлечение идентификатора транзакции (TID), сохраненного в базе данных измерений в соответствии с выбранным идентификатором MID, и формирование запроса, содержащего идентификатор TID, прием ответа от службы измерений, дополнительно содержащего идентификатор TID, и после обработки списка идентификаторов KID в ответе формирование нового идентификатора TID для следующего запроса для идентификатора MID и сохранение сформированного идентификатора TID в базе данных измерений в соответствии с выбранным идентификатором MID для извлечения и использования в связи со следующим запросом для идентификатора MID.

14. Способ передачи накопленных измеренных данных от клиента в службу измерений, при котором каждый набор измеренных данных индксируется в базе данных измерений клиента в соответствии с идентификатором измерений (MID) и дополнительно индексируется в базе данных измерений в соответствии с идентификатором, ассоциированным с содержимым (KID), при этом клиент выбирает конкретный сертификат измерений и определяет из него идентификатор MID, указанный в нем, выбирает по меньшей мере, часть измеренных данных в базе данных измерений, содержащей выбранный идентификатор MID из выбранного сертификата измерений, где выбранные измеренные данные упорядочены в соответствии с идентификатором KID, формирует запрос на основе выбранных измеренных данных и

выбранного сертификата измерений, посылает сформированный запрос в службу измерений, при этом служба измерений получает измеренные данные из запроса, сохраняет их и формирует ответ, который должен быть возвращен клиенту на основании запроса, клиент получает ответ из службы измерений, включающий список идентификаторов KID выбранных данных измерений в запросе, подтверждает, что ответ соответствует запросу, и обрабатывает список идентификаторов KID в ответе путем удаления для каждого идентификатора KID измеренных данных из базы данных измерений, содержащих определенные идентификаторы MID и KID.

15. Способ по п.14, включающий формирование запроса, содержащего идентификатор MID из сертификата измерений, идентификацию местонахождения службы измерений из сертификата измерений, идентификатор транзакции (TID), выбранный для запроса, и выбранные измеренные данные.

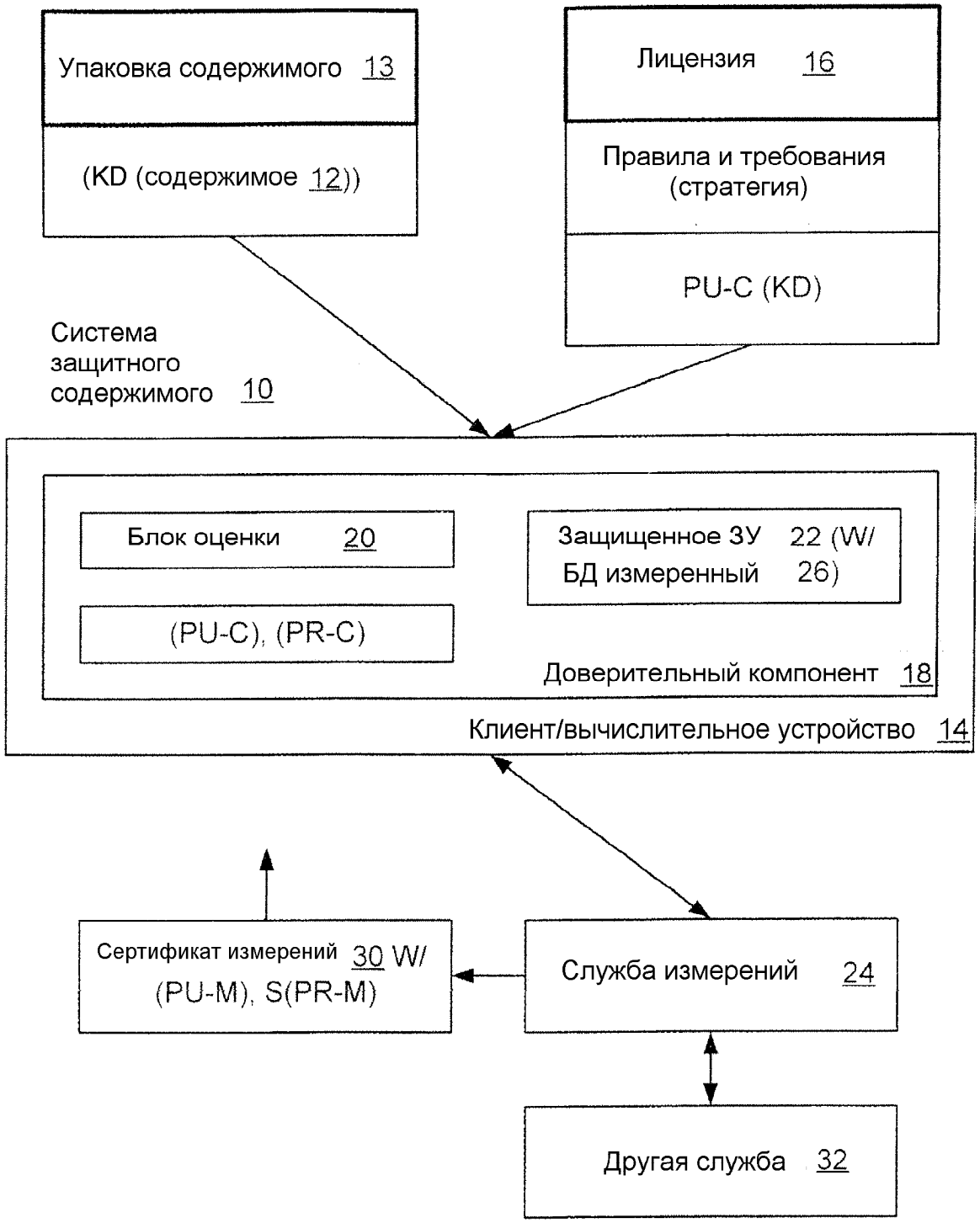
16. Способ по п.15, включающий формирование запроса, содержащего выбранные измеренные данные, зашифрованные в соответствии с симметричным ключом доступа для получения структуры в форме (ключ доступа (данные измерений)), и дополнительно включающего в себя ключ доступа, зашифрованный в соответствии с открытым ключом (PU-M) из сертификата измерений для получения структуры в форме (PU-M (ключ доступа)), причем служба измерений может применить секретный ключ (PR-M), соответствующий ключу (PU-M) к структуре (PU-M(ключ доступа)) из запроса для получения ключа доступа, может применить полученный ключ доступа к структуре (ключ доступа(данные измерений)) из запроса для получения измеренных данных, и может затем сохранить полученные измеренные данные.

17. Способ по п.15, включающий формирование запроса, дополнительно содержащего установленный флаг частичных данных, если клиент не может сформировать запрос, который содержит все накопленные измеренные данные в базе данных измерений для определенного идентификатора MID из ыбранного сертификата измерений.

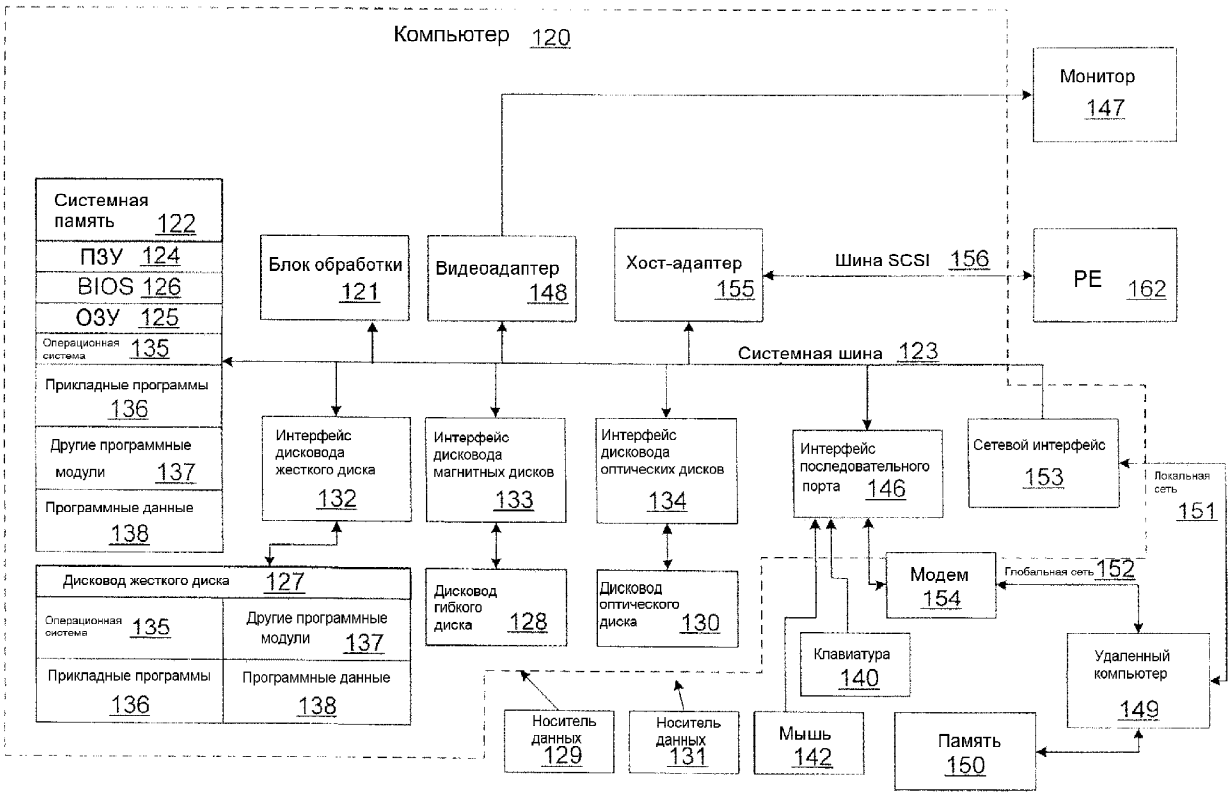
18. Способ по п.14, включающий прием ответа, содержащего идентификатор MID, как было установлено в запросе, идентификатор транзакции (TID), как было установлено в запросе, и, по меньшей мере, часть выбранных измеренных данных, как было установлено в запросе.

19. Способ по п.18, включающий прием ответа, дополнительно содержащего установленный флаг частичных данных, если запрос содержал установленный флаг частичных данных, указывающий на то, что клиент не мог сформировать запрос, содержащий все накопленные измеренные данные в базе данных измерений для определенного идентификатора MID из выбранного сертификата измерений, и что клиент, таким образом, имеет дополнительные измеренные данные для передачи в службу измерений по отношению к определенному идентификатору MID запроса.

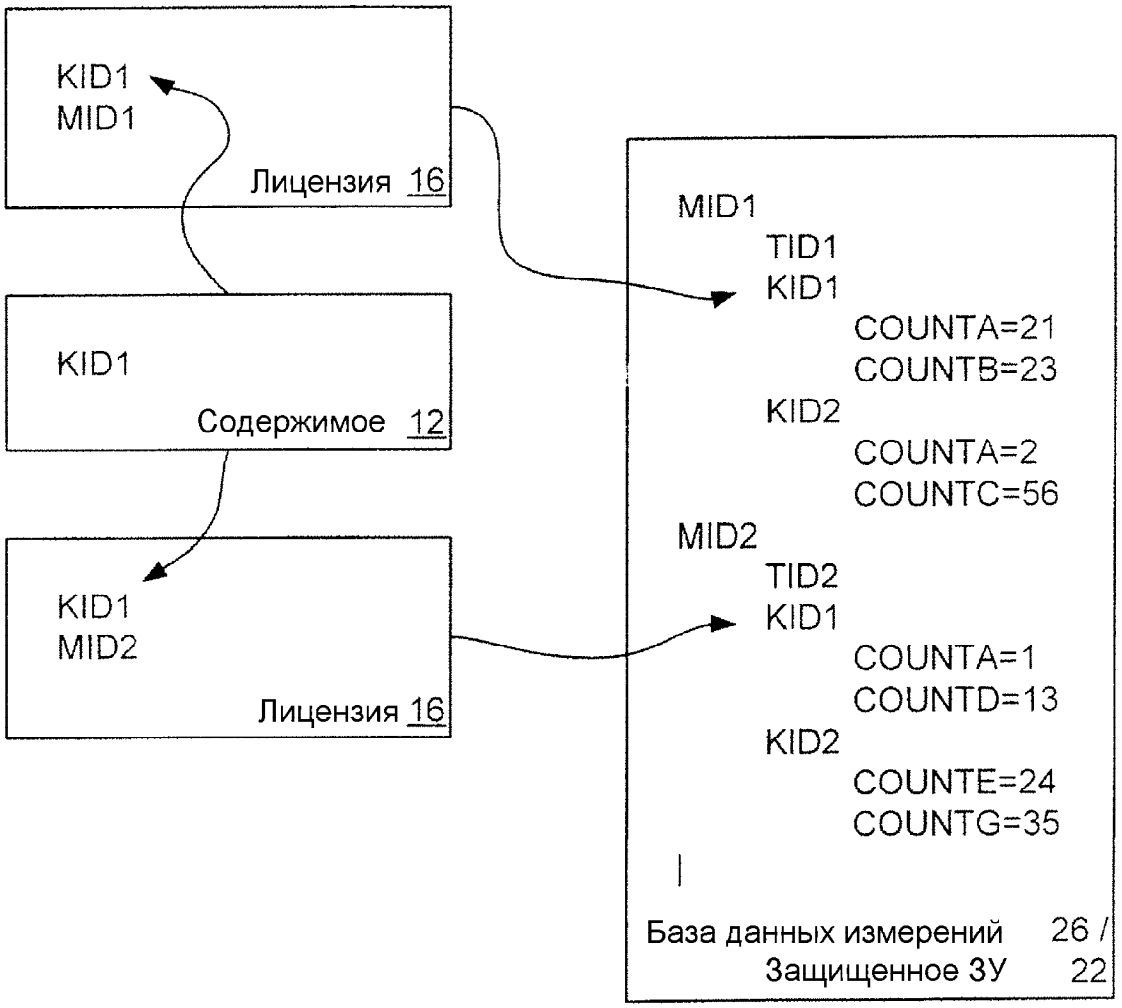
20. Способ по п.19, дополнительно включающий, если ответ содержит установленный флаг частичных данных, выбор, по меньшей мере, части дополнительных измеренных данных в базе данных измерений, имеющих идентификатор MID, определенный из выбранного сертификата измерений, формирование дополнительного запроса на основе выбранных дополнительных измеренных данных и выбранного сертификата измерений; и передачу сформированного дополнительного запроса в службу измерений.


Упаковка содержимого 13
(KD (содержимое 12))
Лицензия 16
Правила и требования (стратегия)
PU-C (KD)
Система защитного содержимого 10
Блок оценки 20
(PU-C), (PR-C)
Защищенное ЗУ 22 (W/ БД измеренный 26)
Доверительный компонент 18
Клиент/вычислительное устройство 14
Сертификат измерений 30 W/ (PU-M), S(PR-M)
Служба измерений 24
Другая служба 32

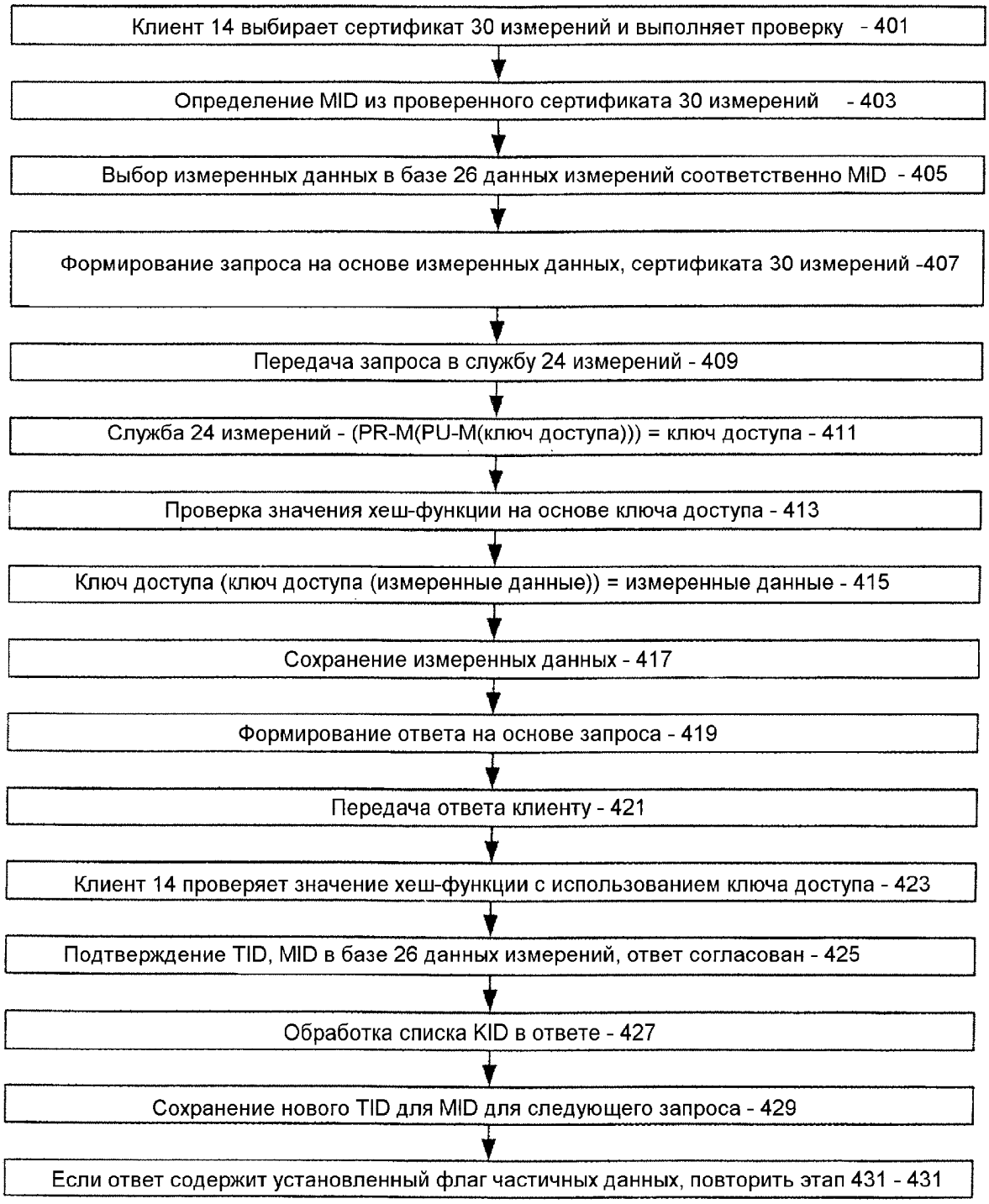
Фиг.1


Компьютер 120
Монитор 147
Системная память 122
ПЗУ 124
BIOS 126
ОЗУ 125
Операционная система 135
Прикладные программы 136
Другие программные модули 137
Программные данные 138
Блок обработки 121
Видеоадаптер 148
Хост-адаптер 155
Шина SCSI 156
PE 162
Системная шина 123
Интерфейс дисковода жесткого диска 132
Интерфейс дисковода магнитных дисков 133
Интерфейс дисковода оптических дисков 134
Интерфейс последовательного порта 146
Сетевой интерфейс 153
Локальная сеть 151
Дисковод жесткого диска 127
Операционная система 135
Другие программные модули 137
Прикладные программы 136
Программные данные 138
Дисковод гибкого диска 128
Дисковод оптического диска 130
Модем 154
Глобальная сеть 152
Клавиатура 140
Удаленный компьютер 149
Носитель данных 129
Носитель данных 131
Мышь 142
Память 150

Фиг.2


KID1
MID1
Лицензия 16
KID1
Содержимое 12
KID1
MID2
Лицензия 16
MID1
TID1
KID1
COUNTA=21
COUNTB=23
KID2
COUNTA=2
COUNTC=56
MID2
TID2
KID1
COUNTA=1
COUNTD=13
KID2
COUNTE=24
COUNTG=35
База данных измерений 26 /
Защищенное ЗУ 22

Фиг.3


Клиент 14 выбирает сертификат 30 измерений и выполняет проверку - 401
Определение MID из проверенного сертификата 30 измерений - 403
Выбор измеренных данных в базе 26 данных измерений соответственно MID - 405
Формирование запроса на основе измеренных данных, сертификата 30 измерений -407
Передача запроса в службу 24 измерений - 409
Служба 24 измерений - (PR-M(PU-M(ключ доступа))) = ключ доступа - 411
Проверка значения хеш-функции на основе ключа доступа - 413
Ключ доступа (ключ доступа (измеренные данные)) = измеренные данные - 415
Сохранение измеренных данных - 417
Формирование ответа на основе запроса - 419
Передача ответа клиенту - 421
Клиент 14 проверяет значение хеш-функции с использованием ключа доступа - 423
Подтверждение TID, MID в базе 26 данных измерений, ответ согласован - 425
Обработка списка KID в ответе - 427
Сохранение нового TID для MID для следующего запроса - 429
Если ответ содержит установленный флаг частичных данных, повторить этап 431 - 431

Фиг.4