РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 348 073** (13) **C2**

(51) МПК
G06F 17/40 (2006.01)
H04L 9/32 (2006.01)
G06F 21/20 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2004105509/09, 24.02.2004**

(24) Дата начала отсчета срока действия патента:
24.02.2004

(30) Конвенционный приоритет:
25.02.2003 US 10/373,458

(43) Дата публикации заявки: **10.08.2005**

(45) Опубликовано: **27.02.2009 Бюл. № 6**

(56) Список документов, цитированных в отчете о поиске: **«Internet X.509 Public Key Infrastructure Certificate Management Protocols», March 1993, 1.2.3, 2.2, 2.2.1.2, 2.2.1.4, 2.2.2.1-2.3.2, 2.4, 2.4.3, 3.1, 3.1.2, 3.3.9, 3.3.10, Приложение B, найдено в Интернет 16.01.2007 (найдено: http://www.ietf.org/rfc/rfc2510.txt). RU 2144269 C1, 10.01.2000. WO 00/58811 A2, 05.10.2000. RU 2183348 C2, 10.06.2002.**

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):
КОСТАЛ Грегори (US),
БОРН Стив (US),
КРИШНАСВАМИ Винай (US)

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

RU 2348073 C2

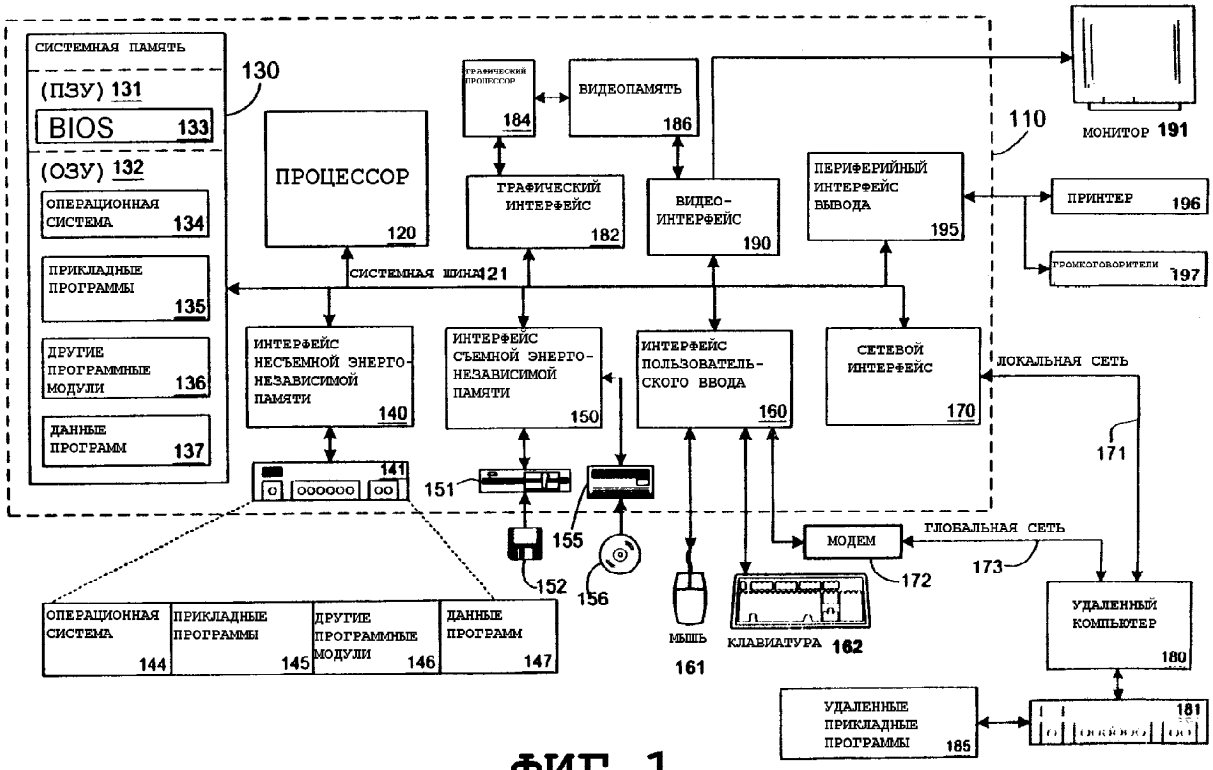
(54) РЕГИСТРАЦИЯ/СУБРЕГИСТРАЦИЯ СЕРВЕРА УПРАВЛЕНИЯ ЦИФРОВЫМИ ПРАВАМИ (УЦП) В АРХИТЕКТУРЕ УЦП

(57) Реферат:

Изобретение относится к системе управления цифровыми правами. Техническим результатом является возможность осуществления контролируемого воспроизведения или проигрывания произвольных форм цифрового контента в среде, где документы совместно используюся определенной группой лиц. (УЦП) имеет множество серверов УЦП, выполняющих функциональные возможности УЦП, и входящий сервер УЦП-В регистрируется в системе посредством регистрирующего сервера УЦП-Р, так что входящий сервер УЦП-В должен быть доверенным в этой системе. Сервер УЦП-В посылает запрос на регистрацию на сервер УЦП-Р, включающий в себя представляющие идентификационные данные и открытый ключ (PU-E). Сервер УЦП-Р проверяет подлинность представляющих идентификационных данных и, если запрос должен быть удовлетворен, генерирует цифровой сертификат регистрации с помощью (PU-E) для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП. Вновь зарегистрированный сервер УЦП-В со сгенерированным сертификатом регистрации может использовать его для выдачи документов с УЦП в системе УЦП. 3 н. и 71 з.п. ф-лы, 17 ил.

RU 2348073 C2

RU 2348073 C2



ФИГ. 1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 348 073** (13) **C2**

(51) Int. Cl.
G06F 17/40 (2006.01)
H04L 9/32 (2006.01)
G06F 21/20 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2004105509/09, 24.02.2004**

(24) Effective date for property rights: **24.02.2004**

(30) Priority:
25.02.2003 US 10/373,458

(43) Application published: **10.08.2005**

(45) Date of publication: **27.02.2009 Bull. 6**

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):
KOSTAL Gregori (US),
BORN Stiv (US),
KRIShNASVAMI Vinaj (US)

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

(54) DIGITAL RIGHTS MANAGEMENT (DRM) SERVER REGISTRATION/SUBREGISTRATION IN DRM ARCHITECTURE

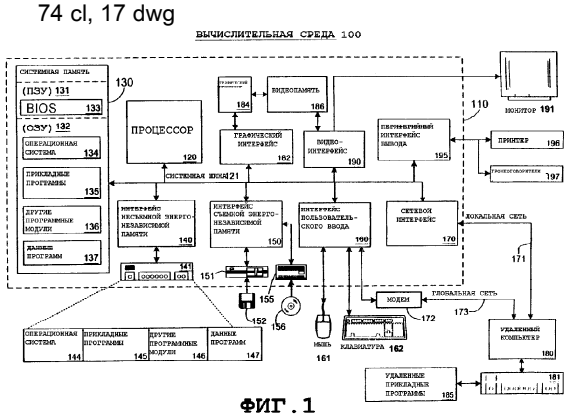
(57) Abstract:

FIELD: physics, computer technology.

SUBSTANCE: invention concerns digital rights management system. (DRM) features multiple DRM servers with DRM functionality, and incoming server DRM-I is registered in the system by registration server DRM-R, so that incoming server DRM-I should be a trust server in this system. DRM-I server sends registration request to DRM-R server including representative identification data and public key (PU-E). DRM-R server checks validity of representative identification data, and if the request can be met, DRM-R server generates digital registration certificate by (PU-E) for DRM-I server for registration of DRM-I server in DRM system. Just registered DRM-I server with generated registration certificate can use it for delivery of documents with DRM in DRM system.

EFFECT: possible controlled reproduction or replay of arbitrary digital content forms in medium where documents are shared by a definite group of users.

74 cl, 17 dwg



RU 2348073 C2

RU 2348073 C2

Перекрестная ссылка на родственные заявки

В следующих заявках на патент США описывается сущность изобретения, которая относится к сущности изобретения настоящей заявки, и они, таким образом, включены в качестве ссылки во всей своей полноте:

заявка на патент США № 10/185 527, поданная 28 июня 2002 г. с кодом патентного поверенного MSFT-1330 и озаглавленная «Obtaining a Signed Rights Label (SRL) for Digital Content and Obtaining a Digital License Corresponding to the Content Based on the SRL in a Digital Rights Management System» (Получение подписанной метки прав (ПМП) для цифрового контента и получение цифровой лицензии, соответствующей контенту, основанному на ПМП, в системе управления цифровыми правами);

заявка на патент США № 10/185 278, поданная 28 июня 2002 г. с кодом патентного поверенного MSFT-1333 и озаглавленная «Using a Rights Template to Obtain a Signed Rights Label (SRL) for Digital Content in a Digital Rights Management System» (Использование шаблона прав для получения подписанной метки прав (ПМП) для цифрового контента в системе управления цифровыми правами);

заявка на патент США № 10/185 511, поданная 28 июня 2002 г. с кодом патентного поверенного MSFT-1343 и озаглавленная «Systems And Methods For Issuing Usage Licenses For Digital Content And Services» (Системы и способы выдачи лицензий на использование для цифрового контента и служб);

заявка на патент США, поданная с кодом патентного поверенного MSFT-1498 и озаглавленная «Publishing Digital Content Within an Organization in Accordance with a Digital Rights Management (DRM) System» (Публикация цифрового контента внутри организации в соответствии с системой управления цифровыми правами (УЦП));

заявка на патент США, поданная с кодом патентного поверенного MSFT-1569 и озаглавленная «Publishing Digital Content Within an Organization in Accordance with a Digital Rights Management (DRM) System» (Публикация цифрового контента внутри организации в соответствии с системой управления цифровыми правами (УЦП)); и

заявка на патент США, поданная одновременно с настоящей заявкой с кодом патентного поверенного MSFT-1537 и озаглавленная «Issuing a Publisher Use License Off-Line in a Digital Rights Management (DRM) System» (Выдача лицензии на использование издателя автономно в системе управления цифровыми правами (УЦП)).

Область техники, к которой относится изобретения

Настоящее изобретение относится к системе управления цифровыми правами (УЦП, DRM). Более конкретно, изобретение относится к использованию системы УЦП для публикации цифрового контента (информационно значимого содержимого) в организации, такой как офис или корпорация и т.п., так что воспроизведение и использование контента внутри организации могут быть ограничены согласно соответствующим правилам использования или условиям лицензии. Еще более конкретно, настоящее изобретение относится к сети серверов УЦП, которые осуществляют подобную систему УЦП, и способу регистрации или субрегистрации сервера УЦП в этой сети.

Предшествующий уровень техники

Управление и принудительное применение цифровых прав крайне желательно в связи с цифровым контентом, таким как цифровое аудио, цифровое видео, цифровой текст, цифровые данные, цифровые мультимедийные данные и т.д., где такой цифровой контент должен быть распространен среди одного или нескольких пользователей. Цифровой контент может быть статическим, таким как, например, текстовый документ, или он может быть потоковым, такой как потоковое аудио/видео реального события. Типичные методы распределения включают в себя материальные устройства, такие как магнитный (флоппи) диск, магнитная лента, оптический (компакт-) диск (CD) и т.д., и нематериальные носители, такие как электронная доска объявлений, электронная сеть, Интернет и т.д. При приеме пользователь воспроизводит или «проигрывает» цифровой контент с помощью соответствующего воспроизводящего устройства, такого как медиаплеер на персональном компьютере или т.п.

При одном сценарии владелец контента или владелец прав, такой как автор, издатель, вещательная компания и т.д., желает распространить такой цифровой контент каждому из многих пользователей или получателей в обмен на лицензионную плату или некоторую другую оплату. При таком сценарии контентом может быть песня, альбом песен, фильм и т.д., и целью распространения является взимание лицензионных плат. Такой владелец контента, при наличии выбора, вероятно, пожелает ограничить то, что пользователь может делать с таким распределенным цифровым контентом. Например, владелец контента может пожелать ограничить копирование пользователем и повторное распространение такого контента второму пользователю, по меньшей мере таким способом, который лишает владельца контента возможности взимать лицензионную плату у такого второго пользователя.

Кроме того, владелец контента может пожелать предоставить пользователю гибкость в покупке лицензий на использование различных типов с различными лицензионными платами, в то же самое время требуя от пользователя соблюдения условий лицензии какого бы ни было типа, которая, фактически, куплена. Например, владелец контента может пожелать разрешить воспроизведение распространяемого цифрового контента только ограниченное количество раз, только в течение некоторого суммарного времени, только на машине определенного типа, только на медиаплеере определенного типа, только пользователям определенного вида и т.д.

При другом сценарии разработчик контента, такой как сотрудник или член организации, желает распространить такой цифровой контент одному или нескольким другим сотрудникам или членам в организации или другим лицам вне организации, но хотел бы удержать других от воспроизведения контента. В данном случае распространение контента более похоже на основанное на организации совместное использование контента конфиденциальным или ограниченным образом, в противоположность свободному распространению в обмен на лицензионную плату или некоторую другую оплату.

При таком сценарии контентом может быть презентация документа, электронная таблица, база данных, электронная почта и т.п., например, обмен которыми может выполняться внутри офисного окружения, и разработчик контента может пожелать гарантировать, чтобы контент оставался внутри организации или офисного окружения и не воспроизводился несанкционированными лицами, такими как, например, конкуренты или противники. Также, такой разработчик контента желает ограничить то, что получатель может делать с таким распространяемым цифровым контентом. Например, владелец контента может пожелать ограничить копирование пользователем и повторное распространение такого контента второму пользователю, по меньшей мере таким способом, который предоставляет контент вне круга пользователей, которым разрешено воспроизводить контент.

Кроме того, разработчик контента может пожелать предоставить различным получателям различные уровни прав на воспроизведение. Например, разработчик контента может пожелать, чтобы защищенный цифровой контент можно было просматривать и нельзя было печатать для одного класса лиц и можно было просматривать и печатать для другого класса лиц.

Однако, и при любом сценарии, после распространения такой владелец/разработчик контента обладает очень незначительным, если вообще обладает, контролем над цифровым контентом. Это особенно проблематично в виду того факта, что практически каждый персональный компьютер включает в себя программное и аппаратное обеспечение, необходимое для выполнения точной цифровой копии такого цифрового контента и загрузки такой точной цифровой копии на записываемый магнитный или оптический диск или передачи любому адресату такой точной цифровой копии по сети, такой как Интернет.

Конечно, как часть транзакции, в которой распространяется контент, владелец/разработчик контента может потребовать, чтобы пользователь/получатель цифрового контента дал обещание не осуществлять повторное распространение такого

цифрового контента нежелательным образом. Однако такое обещание легко дается и легко нарушается. Владелец/разработчик контента может попытаться предотвратить такое повторное распространение посредством любого из нескольких известных устройств защиты, обычно включающих в себя шифрование и дешифрование. Однако, скорее всего, слишком немногое препятствует умеренно решительному пользователю расшифровать зашифрованный цифровой контент, сохранить такой цифровой контент в незашифрованном виде и затем повторно распространить его.

В таком случае существует потребность в создании архитектуры и способа принудительного применения и управления цифровыми правами (УЦП), которые позволяют осуществлять контролируемое воспроизведение или проигрывание произвольных форм цифрового контента, причем такой контроль является гибким и определяемым владельцем/разработчиком такого цифрового контента. Более конкретно, существует потребность в такой архитектуре, которая позволяет и способствует такому контролируемому воспроизведению, особенно в среде офиса или организации и т.п., где документы должны совместно использоваться определенной группой лиц или классов лиц. Еще более конкретно, существует потребность в способе регистрации предоставляющих санкции серверов в архитектуре.

Краткое изложение сущности изобретения

Вышеупомянутые потребности выполняются, по меньшей мере частично, настоящим изобретением, в котором система управления цифровыми правами (УЦП) имеет множество серверов УЦП, выполняющих функциональные возможности УЦП, и входящий сервер УЦП-В (DRM-E) регистрируется в системе посредством регистрирующего сервера УЦП-Р (DRM-R), так что входящий сервер УЦП-В должен быть доверенным в системе. В изобретении сервер УЦП-В обеспечивает пару из открытого/секретного ключей (PU-E, PR-E) для идентификации такого сервера УЦП-В в системе УЦП, обеспечивает представляющие его идентификационные данные и посылает запрос на регистрацию на сервер УЦП-Р, включающий в себя представляющие идентификационные данные и (PU-E).

Сервер УЦП-Р проверяет подлинность представляющих идентификационных данных и, если запрос должен быть удовлетворен, генерирует цифровой сертификат регистрации для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП. Сгенерированный сертификат регистрации основан, по меньшей мере частично, на (PU-E). Сервер УЦП-Р возвращает сгенерированный сертификат регистрации на запрашивающий сервер УЦП-В и вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации в соответствующем месте для будущего использования. Сервер УЦП-В с сертификатом на регистрацию может использовать его для выдачи документов с УЦП в системе УЦП.

Перечень чертежей

Вышеприведенное краткое изложение, а также последующее подробное описание вариантов выполнения настоящего изобретения, легче понять при чтении совместно с прилагаемыми чертежами. С целью иллюстрации изобретения на чертежах показаны варианты выполнения, которые в настоящее время являются предпочтительными. Следует понимать, однако, что изобретение не ограничивается конкретными показанными устройствами и средствами. На чертежах:

фиг.1 - блок-схема, представляющая иллюстративную неограничивающую вычислительную среду, в которой может быть осуществлено настоящее изобретение;

фиг.2 - блок-схема, представляющая иллюстративную сетевую среду, имеющую разнообразные вычислительные устройства, в которой может быть осуществлено настоящее изобретение;

фиг.3 - функциональная блок-схема предпочтительного варианта выполнения системы и способа в соответствии с изобретением для публикации цифрового контента;

фиг.4 - схема последовательности операций предпочтительного варианта выполнения способа в соответствии с изобретением для публикации цифрового контента с управляемыми правами;

фиг.4А - блок-схема, изображающая структуру подписанной метки прав, получаемой способом по фиг.4;

фиг.5 - блок-схема предпочтительного варианта выполнения системы и способа в соответствии с изобретением для лицензирования цифрового контента с управляемыми правами;фиг.6А и 6В - схемы последовательности операций предпочтительного варианта выполнения способа в соответствии с изобретением для лицензирования цифрового контента с управляемыми правами;

фиг.7 - блок-схема, изображающая сертификат, выданный сервером УЦП пользователю, позволяющий пользователю выполнять автономную публикацию в соответствии с одним вариантом выполнения настоящего изобретения;

фиг.8 - блок-схема, изображающая сертификат по фиг.7 вместе с лицензией издателя, которая позволяет публикующему пользователю воспроизводить контент, автономно опубликованный им, в соответствии с одним вариантом выполнения настоящего изобретения;

фиг.9 - схема последовательности операций, изображающая ключевые этапы, выполняемые публикующим пользователем для получения лицензии на публикацию по фиг.8, в соответствии с одним вариантом выполнения настоящего изобретения;

фиг.10 - схема последовательности операций, изображающая ключевые этапы, выполняемые публикующим пользователем для использования полученной лицензии на публикацию по фиг.9 для воспроизведения соответствующего контента в соответствии с одним вариантом выполнения настоящего изобретения;

фиг.11 - блок-схема, изображающая архитектуру принудительного применения примера основанной на доверии системы;

фиг.12 - блок-схема, изображающая множество серверов УЦП, которые могут существовать в архитектуре настоящего изобретения, где каждый (входящий) сервер УЦП регистрируется или субрегистрируется в архитектуре другим (регистрирующим) сервером УЦП, выдающим ему сертификат регистрации;

фиг.13 - блок-схема, изображающая сертификат регистрации по фиг.12 вместе с сертификатом поручительства, представляемым, по меньшей мере в некоторых случаях, входящим сервером УЦП регистрирующему серверу УЦП; и

фиг.14 и 15 - схемы последовательности операций, изображающие ключевые этапы, выполняемые регистрирующими и входящими серверами УЦП по фиг.13 и 14, для регистрации (фиг.14) или субрегистрации (фиг.15) входящего сервера УЦП.

Подробное описание изобретения

Вычислительная среда

Фиг.1 и последующее описание предназначены для того, чтобы предоставить краткое общее описание подходящей вычислительной среды, в которой может быть осуществлено изобретение. Необходимо понять, однако, что карманные, портативные и другие вычислительные устройства всех типов рассматриваются для применения в связи с настоящим изобретением. Хотя ниже описывается компьютер общего назначения, это только один пример, и настоящее изобретение требует только тонкого клиента, имеющего функциональную совместимость и взаимодействие с сетевым сервером. Таким образом, настоящее изобретение может быть реализовано в среде сетевых служб, выполняющих роль ведущих узлов, в которую ресурсы клиента включены в очень малом или минимальном объеме, например сетевой среде, в которой клиентское устройство служит просто в качестве браузера или интерфейса для «Всемирной паутины» (WWW).

Хотя это и не требуется, изобретение может быть осуществлено посредством интерфейса прикладного программирования (API) для использования разработчиком и/или включено в программное обеспечение просмотра ресурсов сети, которое будет описано в общем контексте машиноисполняемых инструкций, таких как программные модули, выполняемые одним или несколькими компьютерами, такими как клиентские рабочие станции, серверы или другие устройства. Вкратце, программные модули включают в себя процедуры, программы, объекты, компоненты, структуры данных и т.п., которые выполняют

определенные задачи или реализуют определенные абстрактные типы данных. Обычно функциональные возможности программных модулей могут быть объединены или распределены, как требуется в различных вариантах выполнения. Кроме того, специалисту в этой области техники понятно, что изобретение может быть реализовано с другими конфигурациями компьютерных систем. Другие общеизвестные вычислительные системы, среды и/или конфигурации, которые могут быть пригодны для использования с изобретением, включают в себя, не в ограничительном смысле, персональные компьютеры (ПК), автоматизированные торговые автоматы, серверные компьютеры, карманные или портативные устройства, мультипроцессорные системы, микропроцессорные системы, программируемую бытовую электронику, сетевые ПК, миникомпьютеры, универсальные компьютеры (мейнфреймы) и т.д. Изобретение также может быть реализовано в распределенных вычислительных средах, где задачи выполняются удаленными устройствами обработки, которые связаны через сеть связи или другую среду передачи данных. В распределенной вычислительной среде программные модули могут быть расположены как на локальных, так и на удаленных носителях данных компьютеров, включая запоминающие устройства.

На фиг.1, таким образом, изображен пример соответствующей среды 100 вычислительной системы, в которой может быть осуществлено изобретение, хотя, как выяснено выше, среда 100 вычислительной системы представляет собой только один пример соответствующей вычислительной среды и не предназначена для того, чтобы налагать какое-либо ограничение в отношение объема использования или функциональных возможностей изобретения. Вычислительная среда 100 также не должна интерпретироваться как имеющая какую-либо зависимость или необходимое условие, относящееся к любому одному компоненту или комбинации компонентов, изображенных в иллюстративной операционной среде 100.

Как показано на фиг.1, иллюстративная система для осуществления изобретения включает в себя вычислительное устройство общего назначения в виде компьютера 110. Компоненты компьютера 110 могут включать в себя, но не в ограничительном смысле, процессор 120, системную память 130 и системную шину 121, которая соединяет различные компоненты системы, включая системную память с процессором 120. Системная шина 121 может быть любого из нескольких типов шинных структур, включающих в себя шину памяти или контроллер памяти, периферийную шину и локальную шину, использующие любую из многочисленных шинных архитектур. В качестве примера, а не ограничения, такие архитектуры включают в себя шину архитектуры промышленного стандарта (ISA), шину микроканальной архитектуры (MCA), усовершенствованную шину ISA (EISA), локальную шину Ассоциации по стандартам в области видеоэлектроники (VESA) и шину межсоединений периферийных компонентов (PSI) (также известную как шина расширения).

Компьютер 110 обычно включает в себя разнообразные машиночитаемые носители. Машиночитаемые носители могут быть любыми доступными носителями, к которым компьютер 110 может осуществить доступ, и включают в себя как энергозависимые, так и энергонезависимые носители, как съемные, так и несъемные носители. В качестве примера, а не ограничения, машиночитаемые носители могут содержать носители данных компьютера и среду передачи данных. Носители данных компьютера включают в себя как энергозависимые, так и энергонезависимые, как съемные, так и несъемные носители, реализованные любым способом или по любой технологии для хранения информации, такой как машиночитаемые команды, структуры данных, программные модули или другие данные. Носители данных компьютера включают в себя, но не в ограничительном смысле, оперативное запоминающее устройство (ОЗУ), постоянное запоминающее устройство (ПЗУ), электрически стираемое программируемое ПЗУ (EEPROM), флэш-память или память, изготовленную по другой технологии, компакт-диск, цифровой универсальный диск (DVD) или другой накопитель на оптическом диске, магнитные кассеты, магнитную ленту, накопитель на магнитном диске или другие магнитные запоминающие устройства, или

любой другой носитель, который может быть использован для хранения требуемой информации и к которому компьютер 110 может осуществить доступ. Среда передачи данных обычно воплощает машиночитаемые команды, структуры данных, программные модули или другие данные в модулированном данными сигнале, таком как несущая волна или другой механизм транспортировки, и включает в себя любую среду доставки информации. Термин «модулированный данными сигнал» подразумевает сигнал, одна или несколько характеристик которого устанавливаются или изменяются так, что они кодируют информацию в сигнале. В качестве примера, а не ограничения, среда передачи данных включает в себя проводную среду, такую как проводная сеть или непосредственное проводное соединение, и беспроводную среду, такую как акустическая, радиочастотная (РЧ), инфракрасная и другая беспроводная среда. Комбинации любых из вышеперечисленных носителей также должны быть включены в сферу рассмотрения машиночитаемых носителей.

Системная память 130 включает в себя носители данных компьютера в виде энергозависимой и/или энергонезависимой памяти, такой как постоянное запоминающее устройство (ПЗУ) 131 и оперативное запоминающее устройство (ОЗУ) 132. Базовая система 133 ввода/вывода (BIOS), содержащая базовые процедуры, которые способствуют передаче информации между элементами внутри компьютера 110, например, во время запуска, обычно хранится в ПЗУ 131. ОЗУ 132 обычно содержит данные и/или программные модули, к которым процессор 120 имеет немедленный доступ и/или которыми процессор 120 оперирует в текущий момент. В качестве примера, а не ограничения, на фиг.1 изображена операционная система 134, прикладные программы 135, другие программные модули 136 и данные 137 программ.

Компьютер 110 также может включать в себя другие съемные/несъемные, энергозависимые/энергонезависимые носители данных компьютера. Только в качестве примера на фиг.1 изображен накопитель 141 на жестких магнитных дисках, который считывает или записывает на несъемный энергонезависимый магнитный носитель, привод 151 магнитного диска, который считывает или записывает на съемный энергонезависимый магнитный диск 152, и привод 155 оптического диска, который считывает или записывает на съемный энергонезависимый оптический диск 156, такой как компакт-диск или другой оптический носитель. Другие съемные/несъемные, энергозависимые/энергонезависимые носители данных компьютера, которые могут быть использованы в иллюстративной операционной среде, включают в себя, но не в ограничительном смысле, кассеты с магнитной лентой, карты флэш-памяти, цифровые универсальные диски, цифровую видеоленту, твердотельное ОЗУ, твердотельное ПЗУ и т.п. Накопитель 141 на жестких магнитных дисках обычно подсоединен к системной шине 121 через интерфейс несъемной памяти, такой как интерфейс 140, а привод 151 магнитного диска и привод 155 оптического диска обычно подсоединены к системной шине 121 посредством интерфейса съемной памяти, такого как интерфейс 150.

Приводы и связанные с ними носители данных компьютера, описанные выше и изображенные на фиг.1, обеспечивают хранение машиночитаемых команд, структур данных, программных модулей и других данных для компьютера 110. На фиг.1, например, накопитель 141 на жестких магнитных дисках изображен как хранящий операционную систему 144, прикладные программы 145, другие программные модули 146 и данные 147 программ. Следует отметить, что эти компоненты могут быть либо теми же, либо отличными от операционной системы 134, прикладных программ 135, других программных модулей 136 и данных 137 программ. Операционной системе 144, прикладным программам 145, другим программным модулям 146 и данным 147 программ здесь даны другие номера, чтобы показать, что, как минимум, они являются другими копиями. Пользователь может вводить команды и информацию в компьютер 110 через устройства ввода, такие как клавиатура 162 и указательное устройство 161, обычно упоминаемое как мышь, шаровой манипулятор или сенсорная панель. Другие устройства ввода (не показаны) могут включать в себя микрофон, джойстик, игровой планшет, антенну спутниковой связи,

сканер или т.п. Эти и другие устройства ввода часто подключаются к процессору 120 через интерфейс 160 пользовательского ввода, который подсоединен к системной шине 121, но может быть подсоединен посредством другого интерфейса и шинных структур, таких как параллельный порт, игровой порт или универсальная последовательная шина (USB).

Монитор 191 или устройство отображения другого типа также подсоединено к системной шине 121 через интерфейс, такой как видеоинтерфейс 190. Графический интерфейс 182, такой как северный мост, также может быть подсоединен к системной шине 121. Северный мост представляет собой набор микросхем, который организует связь с центральным или главным процессором (CPU) 120 и отвечает за обмен данными с ускоренным графическим портом (AGP). Один или несколько графических процессоров (GPU) 184 могут обмениваться данными с графическим интерфейсом 182. В этом отношении процессоры GPU 184, в основном, включают в себя память на кристалле, такую как регистровая память, и процессоры GPU 184 обмениваются данными с видеопамятью 186. Процессоры GPU 184, однако, представляют собой только один пример сопроцессора и, таким образом, многочисленные сопроцессорные устройства могут быть включены в компьютер 110. Монитор 191 или устройство отображения другого типа также подсоединяется к системной шине 121 через интерфейс, такой как видеоинтерфейс 190, который, в свою очередь, может обмениваться данными с видеопамятью 186. В дополнение к монитору 191 компьютеры также могут включать в себя другие периферийные устройства вывода, такие как громкоговорители 197 и принтер 196, которые могут быть подсоединены через периферийный интерфейс 195 вывода.

Компьютер 110 может работать в сетевой среде, используя логические соединения с одним или несколькими удаленными компьютерами, такими как удаленный компьютер 180. Удаленным компьютером 180 может быть персональный компьютер, сервер, маршрутизатор, сетевой ПК, одноранговое устройство или другой общий узел сети, и он обычно включает в себя многие или все из элементов, описанных выше в отношении компьютера 110, хотя на фиг.1 изображено только запоминающее устройство 181. Логические соединения, изображенные на фиг.1, включают в себя локальную сеть (ЛС) 171 и глобальную сеть (ГС) 173, но также могут включать в себя другие сети. Такие сетевые среды распространены в офисах, компьютерных сетях масштаба предприятия, интрасетях и сети Интернет.

При использовании в сетевой среде ЛС компьютер 110 подключается к ЛС 171 через сетевой интерфейс или адаптер 170. При использовании в сетевой среде ГС компьютер 110 обычно включает в себя модем 172 или другое средство для установления связи через ГС 173, такую как Интернет. Модем 172, который может быть внутренним или внешним, может быть подсоединен к системной шине 121 через интерфейс 160 пользовательского ввода, или другой соответствующий механизм. В сетевой среде программные модули, описанные в отношении компьютера 110, или его частей, могут храниться на удаленном запоминающем устройстве. В качестве примера, а не ограничения, на фиг.1 изображены удаленные прикладные программы 185, постоянно находящиеся на запоминающем устройстве 181. Понятно, что показанные сетевые соединения являются примерными, и могут быть использованы другие средства установления линии связи между компьютерами.

Специалисту в этой области техники понятно, что компьютер 110 или другое клиентское устройство могут использоваться в качестве части компьютерной сети. В этом отношении настоящее изобретение относится к любой компьютерной системе, имеющей любое количество блоков памяти или запоминающих устройств и любое количество приложений и процессов, происходящих в любом количестве запоминающих устройств или томов. Настоящее изобретение может применяться к среде с серверными компьютерами и клиентскими компьютерами, используемыми в сетевой среде, имеющей удаленное или локальное запоминающее устройство. Настоящее изобретение также может быть применено к автономному вычислительному устройству, имеющему связанные с языками программирования функциональные возможности интерпретации и выполнения.

Распределенное вычисление способствует совместному использованию компьютерных ресурсов и служб посредством непосредственного обмена между вычислительными устройствами и системами. Эти ресурсы и службы включают в себя обмен информацией, кэш-память и дисковое запоминающее устройство для файлов. Распределенное вычисление использует преимущество связности узлов в сети, позволяющее клиентам по-новому применять их совокупную производительность, принося пользу для всего предприятия. В этом отношении многочисленные устройства могут иметь приложения, объекты или ресурсы, которые могут взаимодействовать, чтобы заключать в себе методики аутентификации (установления подлинности) настоящего изобретения для доверяемого графического конвейера(ов).

На фиг.2 представлена блок-схема иллюстративной сетевой или распределенной вычислительной среды. Распределенная вычислительная среда содержит вычислительные объекты 10a, 10b и т.д. и вычислительные объекты или устройства 110a, 110b, 110c и т.д. Эти объекты могут содержать программы, методы, хранилища данных, программируемую логику и т.д. Объекты могут содержать их части или другие устройства, такие как персональные цифровые информационные устройства (PDA), телевизоры, проигрыватели MP3, персональные компьютеры и т.д. Каждый объект может обмениваться данными с другим объектом посредством сети 14 связи. Эта сеть сама может содержать другие вычислительные объекты и вычислительные устройства, которые обеспечивают службы для системы по фиг.2. В соответствии с аспектом изобретения каждый объект 10 или 110 может содержать приложение, которое может запросить методики аутентификации настоящего изобретения для доверяемого графического конвейера(ов).

Также очевидно, что объект, такой как 110c, может находиться на другом вычислительном устройстве 10 или 110. Таким образом, хотя описанная физическая среда может изображать подсоединенные устройства в виде компьютеров, такая иллюстрация является просто примерной, и физическая среда, альтернативно, может быть описана или изображена как содержащая различные цифровые устройства, такие как PDA, телевизоры, проигрыватели MP3 и т.д., программные объекты, такие как интерфейсы, объекты модели компонентных объектов (COM) и т.п.

Существуют многочисленные системы, компоненты и сетевые конфигурации, которые поддерживают распределенные вычислительные среды. Например, вычислительные системы могут быть соединены вместе посредством проводных или беспроводных систем, локальных сетей или распределенных сетей большого масштаба. В настоящее время многие сети соединены с сетью Интернет, которая обеспечивает инфраструктуру для глобальных распределенных вычислений и охватывает многие различные сети.

В домашних сетевых средах существует по меньшей мере четыре отдельные сетевые транспортные среды, каждая из которых может поддерживать уникальный протокол, такие как линия электропитания, среда передачи данных (как беспроводная, так и проводная), среда передачи речи (например, телефонная линия) и среда передачи развлекательной информации. Большинство домашних устройств управления, таких как выключатели света и приборы, могут использовать линию электропитания для установления соединения. Службы передачи данных могут быть подведены к дому посредством широкополосной линии (например, либо посредством цифровой абонентской линии (DSL), либо посредством кабельного модема) и могут быть доступны дома с использованием либо беспроводных (например, HomeRF или 802.11b), либо проводных (например, сетевого приложения по домашней телефонной линии (Home PNA), кат. 5, даже линии электропитания) соединений. Речевой трафик может поступать в дом либо проводным (например, кат. 3), либо беспроводным (например сотовые телефоны) путем и может распределяться по дому, используя проводку кат. 3. Среда передачи развлекательной информации может быть подведена к дому либо через спутник, либо по кабелю и обычно распределяется по дому, используя коаксиальный кабель. Появившиеся интерфейс IEEE 1394 и цифровой видеоинтерфейс (DVI) также представляют собой цифровое межсоединение для кластеров медиаустройств. Все эти сетевые среды и другие среды, которые могут появиться в

качестве стандартов протоколов, могут быть соединены между собой, образуя интрасеть, которая может быть соединена с внешним миром посредством сети Интернет. Вкратце, существуют многочисленные отдельные источники для хранения и передачи данных, и, следовательно, продвигаясь вперед, вычислительные устройства потребуют защиты контента на всех частях конвейера обработки данных.

«Интернет», как правило, относится к совокупности сетей и шлюзов, использующих стек протоколов TCP/IP, которые хорошо известны в области техники, связанной с компьютерными сетями. TCP/IP представляет собой сокращение для «протокола управления передачей/Интернет-протокола». Интернет может быть описан как система географически распределенных удаленных компьютерных сетей, соединенных между собой компьютерами, выполняющими сетевые протоколы, которые позволяют пользователям взаимодействовать и совместно использовать информацию в сетях. Таким образом, вследствие такого глобального совместного использования информации удаленные сети, такие как Интернет, в значительной степени эволюционировали в открытую систему, для которой разработчики могут проектировать приложения программного обеспечения для выполнения специальных операций или служб, по существу без ограничения.

Таким образом, сетевая инфраструктура позволяет получить множество сетевых топологий, таких как архитектура клиент/сервер, одноранговая архитектура или гибридная архитектура. «Клиентом» является член класса или группы, который использует услуги, представляемые другим классом или группой, с которой он не связан. Таким образом, при вычислении клиентом является процесс, т.е. грубо говоря, набор команд или задач, который запрашивает услугу, предоставляемую другой программой. Клиентский процесс использует запрашиваемую услугу без необходимости «знания» любых рабочих подробностей другой программы или самой услуги службы. В архитектуре клиент/сервер, особенно в сетевой системе, клиентом обычно является компьютер, который обращается к совместно используемым сетевым ресурсам, предлагаемым другим компьютером, например сервером. В примере по фиг.2 компьютеры 110a, 110b и т.д. могут рассматриваться как клиенты, а компьютеры 10a, 10b и т.д. могут рассматриваться как сервер, где сервер 10a, 10b и т.д. хранит данные, которые затем дублируются на клиентских компьютерах 110a, 110b и т.д.

Сервером обычно является удаленная компьютерная система, доступная по удаленной сети, такой как Интернет. Клиентский процесс, который может быть активным в первой компьютерной системе, и серверный процесс, который может быть активным во второй компьютерной системе, обмениваются данными между собой по среде передачи данных, таким образом обеспечивая распределенные функциональные возможности и позволяя многочисленным клиентам воспользоваться возможностями сбора информации сервера.

Клиент и сервер обмениваются данными между собой, используя функциональные возможности, обеспечиваемые уровнем протокола. Например, протокол передачи гипертекста (HTTP) представляет собой общий протокол, который используется совместно со Всемирной паутиной (WWW). Обычно сетевой адрес компьютера, такой как унифицированный указатель ресурса (URL), или адрес Интернет-протокола (IP) используется для взаимной идентификации серверного или клиентского компьютера. На сетевой адрес можно ссылаться как на адрес унифицированного указателя ресурса. Например, обмен данными может обеспечиваться по среде связи. В частности, клиент и сервер могут быть соединены друг с другом по соединениям TCP/IP для обмена данными с высокой пропускной способностью.

Таким образом, на фиг.2 изображена иллюстративная сетевая или распределенная среда с сервером, с осуществляющим обмен данными с клиентскими компьютерами по сети/шине, в котором может быть осуществлено настоящее изобретение. Более подробно, ряд серверов 10a, 10b и т.д. соединены сетью/шиной 14 связи, которой может быть ЛС, ГС, интрасеть, Интернет и т.д., с рядом клиентских или удаленных вычислительных устройств 110a, 110b, 110c, 110d, 110e и т.д., таких как портативный компьютер,

карманный компьютер, тонкий клиент, сетевой прибор или другое устройство, такое как кассетный видеомагнитофон, телевизор, печь, лампа, нагреватель и т.п. в соответствии с настоящим изобретением. Таким образом, считается, что настоящее изобретение может быть применено к любому вычислительному устройству, в отношении которого желательно обрабатывать, хранить или воспроизводить защищенный контент из доверяемого источника.

В сетевой среде, в которой сетью/шиной 14 связи является Интернет, например, серверами 10 могут быть веб-серверы, с которыми клиенты 110a, 110b, 110c, 110d, 110e и т.д. обмениваются данными по любому из ряда известных протоколов, таких как HTTP. Серверы 10 также могут служить в качестве клиентов 110, что может быть особенностью распределенной вычислительной среды. Обмен данных может осуществляться проводным или беспроводным путем по необходимости. Клиентские устройства 110 могут обмениваться или не обмениваться данными по сети/шине 14 связи и могут иметь независимый обмен данными, связанный с ними. Например, в случае телевизора или кассетного видеомагнитофона, может присутствовать или отсутствовать аспект сетевого управления ими. Каждый клиентский компьютер 110 или серверный компьютер 10 может быть оснащен различными прикладными программными модулями или объектами 135 и соединениями или доступом к запоминающим элементам или объектам различного типа, на которых могут храниться файлы или на которые может быть загружена или перемещена часть(и) файлов. Таким образом, настоящее изобретение может быть использовано в компьютерной сетевой среде, имеющей клиентские компьютеры 110a, 110b и т.д., которые могут осуществлять доступ к компьютерной сети/шине 14 и взаимодействовать с ней, и серверные компьютеры 10a, 10b и т.д., которые могут взаимодействовать с клиентскими компьютерами 110a, 110b и т. д. и другими устройствами 111 и базами 20 данных.

Обзор управления цифровыми правами (УЦП)

Как известно, и ссылаясь теперь на фиг.11, принудительное применение и управление цифровыми правами (УЦП) в значительной степени желательны в связи с цифровым контентом 12, таким как цифровое аудио, цифровое видео, цифровой текст, цифровые данные, цифровые данные мультимедиа и т.д., где такой цифровой контент 12 должен распространяться среди пользователей. При приеме пользователь воспроизводит или «проигрывает» цифровой контент с помощью соответствующего воспроизводящего устройства, такого как медиаплеер на персональном компьютере 14 или т.п.

Обычно владелец или разработчик (ниже «владелец») контента, распространяющий такой цифровой контент 12, желает ограничить то, что пользователь может делать с таким распространяемым цифровым контентом 12. Например, владелец контента может пожелать ограничить копирование пользователем и повторное распространение такого контента 12 второму пользователю или может пожелать, чтобы распространяемый цифровой контент 12 мог проигрываться только ограниченное число раз, только в течение некоторого суммарного времени, только на машине определенного типа, только на медиаплеере определенного типа, только пользователем определенного вида и т.д.

Однако после того как произошло распространение, такой владелец контента очень слабо контролирует, если вообще контролирует, цифровой контент 12. Система 10 УЦП, в этом случае, позволяет производить контролируемое воспроизведение или проигрывание цифрового контента 12 в произвольных формах, где такой контроль является гибким и определяемым владельцем контента такого цифрового контента. Обычно контент 12 доставляется пользователю в виде комплекта 13 посредством любого подходящего канала распространения. Распространяемый комплект 13 цифрового контента может включать в себя цифровой контент 12, зашифрованный симметричным ключом шифрования/дешифрования (KD), (т.е. (KD(CONTENT))), а также другую информацию, идентифицирующую контент, как получить лицензию на такой контент и т.д.

Основанная на доверии система 10 УЦП позволяет владельцу цифрового контента 12 определить правила лицензии, которые должны быть выполнены до того, как будет разрешено воспроизводить такой цифровой контент 12 на вычислительном устройстве 14

пользователя. Такие правила лицензии могут включать в себя вышеупомянутое временное требование и могут быть реализованы в цифровой лицензии или документе 16 на использование (ниже «лицензия»), которую пользователь/вычислительное устройство 14 пользователя (ниже такие термины являются взаимозаменяемыми, если только обстоятельства не требуют противоположного) должен получить от владельца контента или его посредника. Такая лицензия 16 также включает в себя ключ дешифрования (KD) для дешифрования цифрового контента, зашифрованного, возможно, согласно ключу, дешифруемому вычислительным устройством пользователя.

Владелец контента для порции цифрового контента 12 должен доверять тому, что вычислительное устройство 14 пользователя будет придерживаться правил и требований, определенных таким владельцем контента в лицензии 16, т.е. что цифровой контент 12 не будет воспроизводиться, если не выполняются правила и требования в лицензии 16. В этом случае вычислительное устройство 14 пользователя, предпочтительно, обеспечено доверенным компонентом или средством 18, который не будет воспроизводить цифровой контент 12, кроме как согласно правилам лицензии, содержащимся в лицензии 16, связанной с цифровым контентом 12 и получаемой пользователем.

Доверенный компонент 18 обычно имеет анализатор 20 лицензии, который определяет, является ли лицензия 16 подлинной, анализирует правила и требования лицензии в такой подлинной лицензии 16 и, помимо этого, определяет, основываясь на проанализированных правилах и требованиях лицензии, имеет ли запрашивающий пользователь право на воспроизведение запрашиваемого цифрового контента 12 желаемым образом. Следует понимать, что анализатор 20 лицензии является доверенным в системе 10 УЦП для выполнения пожеланий владельца цифрового контента 12 согласно правилам и требованиям в лицензии 16, и пользователь не должен иметь возможности легкого изменения такого доверенного элемента для любого назначения, нечестного или иного.

Следует понимать, что правила и требования в лицензии 16 могут определять то, имеет ли пользователь права на воспроизведение цифрового контента 12, основываясь на любом из нескольких факторов, включающих в себя: кем является пользователь, где находится пользователь, какой тип вычислительного устройства использует пользователь, какое приложение воспроизведения вызывает систему УЦП, дату, время и т.д. Кроме того, правила и требования лицензии 16 могут ограничивать лицензию 16, например, предварительно определенным числом проигрываний или предварительно определенным временем проигрывания.

Правила и требования могут быть определены в лицензии 16 в соответствии с любым подходящим языком и синтаксисом. Например, язык может просто определять атрибуты и значения, которые должны выполняться (DATE (дата), например, должна быть более поздняя, чем X) или может потребовать выполнение функций согласно определенному сценарию (IF DATE (если дата), например, больше, чем X, THEN DO (тогда выполнить) ...).

После определения анализатором 20 лицензии того, что лицензия 16 является подлинной и что пользователь удовлетворяет правилам и требованиям в ней, цифровой контент 12 может быть воспроизведен. В частности, для воспроизведения контента 12 ключ дешифрования (KD) получают из лицензии 12 и применяют к (KD(CONTENT)) из комплекта 13 контента, в результате чего получают фактический контент 12, и фактический контент 12 затем воспроизводят.

Публикация цифрового контента

На фиг.3 представлена функциональная блок-схема системы и способа для публикации цифрового контента. Термин «публикация» в том виде, в каком он здесь используется, относится к процессу, которому приложение или служба следует, чтобы установить с доверенным объектом набор прав и условий, которые этот объект может выдать для этого контента, а также кому эти права и условия могут быть выданы. В соответствии с изобретением, процесс публикации включает в себя шифрование цифрового контента и связывание списка постоянных принудительно применяемых прав, которые автор контента предполагал для всех возможных пользователей контента. Этот процесс может быть

выполнен безопасным образом, чтобы запретить доступ к любому из прав или контенту, если это не предполагается автором контента.

В частности, используются три объекта для публикации защищенного цифрового контента: приложение 302 подготовки контента, которое выполняется на клиенте 300 и готовит контент для публикации, интерфейс 306 прикладного программирования (API) управления цифровыми правами (УЦП), который также постоянно находится на клиентском устройстве 300, и сервер 320 УЦП, который соединен с возможностью обмена данными с клиентом 300 по сети 330 связи, такой как Интернет, локальная или глобальная сеть или их комбинация. Приложением 302 подготовки контента может быть любое приложение, которое создает цифровой контент. Например, приложением 302 может быть текстовый процессор или другое издательское средство, которое создает цифровые текстовые файлы, цифровую музыку, видео или другой подобный контент. Контент также может включать в себя потоковый контент, такой как потоковое аудио/видео, например, реального события или события, записанного на пленку. Приложение 302 обеспечено криптографическим ключом для шифрования цифрового контента, таким образом формируя файл 304 зашифрованного цифрового контента, и пользователь предоставляет данные о правах, которые должны быть непосредственно связаны с зашифрованным контентом в файле 304 цифрового контента. Данные о правах включают в себя идентификационные данные для каждого объекта, который имеет права в цифровом контенте, и набор прав и условий для каждого идентифицированного объекта.

Таким объектом может быть, например, пользователь, класс пользователей или устройство. Такие права могут включать в себя право на чтение, редактирование, копирование, печать и т.д. цифрового контента. Условия могут включать в себя минимальные системные требования, ограничения по дате и времени, число проигрываний и т.п.

Клиентский API 306 передает зашифрованный цифровой контент и данные о правах на сервер 320 УЦП. Используя процесс, который подробно описан ниже, сервер 320 УЦП определяет, может ли он принудительно применить данные о правах, и, если это так, то сервер 320 УЦП подписывает данные о правах, формируя подписанную метку 308 прав (ПМП, SRL). Вообще говоря, любой доверенный объект может подписать данные о правах, предпочтительно используя ключ, которому доверяет сервер 320 УЦП. Например, клиент может подписать данные о правах, используя ключ, предоставляемый ему сервером 320 УЦП.

Метка 308 прав может включать в себя данные, представляющие описание прав, зашифрованный ключ контента и цифровую подпись на описание прав и зашифрованный ключ контента. Если сервер 320 УЦП подписывает метку прав, то он передает подписанную метку 308 прав обратно клиенту через клиентский API 306, который сохраняет подписанную метку 308 прав на клиентском устройстве 300. Приложение 302 подготовки контента затем связывает подписанную метку 308 прав с файлом 304 зашифрованного цифрового контента, например, посредством сцепления, формируя файл 310 контента с управляемыми правами. Следует отметить, впрочем, что ПМП 308 может храниться в известном месте отдельно от файла 304 контента со ссылкой на ПМП 308, сцепленную с файлом 304 контента, формируя файл 310 контента.

На фиг.4 показан один способ публикации цифрового контента с управляемыми правами. На этапе 402 приложение 302 генерирует ключ контента (СК), который используется для шифрования цифрового контента. Ключ контента (СК) обычно представляет собой симметричный ключ, хотя любой ключ может быть использован для шифрования цифрового контента. Как известно, симметричный ключ используется алгоритмом симметричного ключа как для шифрования, так и для дешифрования. Следовательно, (СК) должен быть хорошо скрыт при совместном использовании отправителем и получателем.На этапе 404 приложение 302 шифрует цифровой контент при помощи (СК), формируя зашифрованный цифровой контент 304 (т.е. (СК(content))). Кроме того, генерируются данные о правах, соответствующие (СК(content)), либо

издателем контента, либо другим объектом. Следует отметить, что такими данными о правах могут быть данные о правах, устанавливаемые на индивидуальной основе, или данные о правах, полученные из предварительно определенного шаблона. Как было описано выше, данные о правах могут включать в себя список объектов, которым будет дано право потреблять контент, конкретные права, которыми владеет каждый из объектов в отношении контента, и любые условия, которые могут быть наложены на эти права.

На этапе 406 API 306 генерирует второй ключ (К2) шифрования, который используется для шифрования ключа (СК) контента. Предпочтительно, (К2) также представляет собой симметричный ключ. На этапе 408 API 306 шифрует (СК) с помощью (К2), получая в результате (К2(СК)). На этапе 410 API 306 сбрасывает (СК), в результате чего (СК) может быть получен только посредством дешифрования (К2(СК)). Чтобы гарантировать, что (СК(content)) защищен центральным сервером 320 УЦП и что все «запросы на лицензии» для контента выполняются централизованным образом в соответствии с данными о правах, API 306 на этапе 412 обращается к обеспеченному серверу 320 УЦП и извлекает его открытый ключ (PU-DRM). На этапе 414 API 306 шифрует (К2) с помощью (PU-DRM), получая в результате (PU-DRM(K2)). Таким образом, (СК) может быть защищен (PU-DRM), чтобы гарантировать, что сервер 320 УЦП является единственным объектом, который может получить доступ к (СК), что требуется для дешифровки (СК(content)). На этапе 416 API 306 шифрует данные о правах (т.е. список санкционированных объектов и соответствующих прав и условий, связанных с каждым санкционированным объектом в списке) с помощью (К2), получая в результате (К2(rightsdata)).

В альтернативном варианте выполнения (СК) может быть использован для непосредственного шифрования данных о правах, получая в результате (СК(rightsdata)), и (PU-DRM) может быть использован для непосредственного шифрования (СК), получая в результате (PU-DRM(СК)), тем самым полностью отказываясь от использования (К2). Однако использование (К2) для шифрования данных о правах и (СК) допускает, что такой (К2) соответствует любому конкретному алгоритму, который может быть подчиняющимся серверу УЦП, тогда как (СК) может быть задан объектом, независимым от сервера УЦП, и может не быть подчиняющимся ему.

На этапе 418 приложение 302 защиты контента представляет (PU-DRM(K2)) и (К2(rightsdata)) на сервер 320 УЦП в качестве метки прав для подписания. Альтернативно, сам клиент может подписать данные о правах так, как изложено ниже. Если данные о правах представляются серверу для подписания, то тогда на этапе 420 сервер 320 УЦП осуществляет доступ к данным о правах и проверяет, что он может принудительно применить права и условия в представленной метке прав. Для проверки того, что он может принудительно применить данные о правах, сервер 320 УЦП применяет секретный ключ (PR-DRM), соответствующий (PU-DRM), к (PU-DRM(K2)), получая в результате (К2), и затем применяет (К2) к (К2(rightsdata)), получая в результате данные о правах в открытом виде. Сервер 320 затем может выполнить любые проверки политик, чтобы проверить, что пользователи, права и условия, определенные в данных о правах, находятся в пределах любой политики, принудительно применяемой сервером 320. Сервер 320 подписывает первоначально представленную метку прав, включающую в себя (PU-DRM(K2)) и (К2(rightsdata)), получая в результате подписанную метку 308 прав (ПМП), где подпись основана на секретном ключе сервера 320 УЦП (PR-DRM), и возвращает ПМП 308 обратно API 306, который затем представляет возвращенную ПМП 308 клиентскому приложению 302.

ПМП 308 представляет собой документ с цифровой подписью, что делает его защищенным от несанкционированного вмешательства. Кроме того, ПМП 308 не зависит от типа фактического ключа и алгоритма, используемых для шифрования контента, но поддерживает сильное однозначное соответствие с контентом, который она защищает. Ссылаясь теперь на фиг.4А, в одном варианте выполнения настоящего изобретения ПМП 308 может включать в себя информацию о контенте, которая является базовым компонентом ПМП 308, включая в себя, возможно, идентификатор контента; информацию о

сервере УЦП, который подписывает ПМП 308, включающую (PU-DRM(K2)) и ссылочную информацию, такую как URL, для определения местоположения сервера УЦП в сети, и информацию о возврате в исходное состояние, если URL приводит к неудаче; информацию, описывающую саму ПМП 308; (K2(rightsdata)):(K2(CK)); и, помимо всего прочего, цифровую подпись (S(PR-DRM)).

Посредством гарантирования того, что доверяемый объект подписывает данные о правах для создания подписанной метки 308 прав, сервер 320 УЦП предполагает, что он выдаст лицензии на контент в соответствии с условиями, изложенными издателем, как описано в данных о правах метки 308 прав. Следует понимать, что пользователю необходимо получить лицензию на воспроизведение контента, особенно ввиду того, что лицензия содержит ключ (СК) контента. Когда пользователь хочет получить лицензию на зашифрованный контент, пользователь может представить запрос на лицензию, включающий в себя ПМП 308 для контента и сертификат, удостоверяющий мандат (учетную запись с параметрами доступа пользователя, сформированными после его успешной аутентификации) пользователя, серверу 320 УЦП или другому выдающему лицензию объекту. Выдающий лицензию объект затем может дешифровать (PU-DRM(K2)) и (K2(rightsdata)) для получения данных о правах, списка всех прав, предоставленных автором (если они есть) запрашивающему лицензию объекту, и составления лицензии только с этими конкретными правами.

Как изложено выше, после приема приложением 302 ПМП 308 такое приложение 302 сцепляет подписанную метку 308 прав с соответствующим (CK(content)) 304, формируя цифровой контент с управляемыми правами. Альтернативно, данные о правах хранятся в известном месте со ссылкой на это место, обеспечиваемой вместе с зашифрованным цифровым контентом. Таким образом, воспроизводящее приложение, поддерживающее УЦП, может обнаружить подписанную метку 308 прав посредством порции контента, которую воспроизводящее приложение пытается воспроизвести. По этому обнаружению запускается воспроизводящее приложение для инициирования запроса лицензии у сервера 320 лицензирования УЦП. Приложение 302 публикации, например, может хранить URL на сервере 320 лицензирования УЦП, или сервер 320 лицензирования УЦП может внедрить свой собственный URL в виде порции метаданных в метку прав перед ее подписью цифровым образом, так что клиентское API 306 УЦП, вызванное воспроизводящим приложением, может идентифицировать корректный сервер 320 лицензирования УЦП.

Получение лицензии на опубликованный контент

На фиг.5 показана система и способ лицензирования цифрового контента с управляемыми правами. Термин «лицензирование» в том виде, в каком он здесь используется, относится к процессу, которому следует приложение или служба для запроса и приема лицензии, которая позволяет объекту, указанному в лицензии, потреблять контент в соответствии с условиями, определенными в лицензии. Входные данные для процесса лицензирования могут включать в себя подписанную метку 308 прав (ПМП), связанную с контентом, для которого запрашивается лицензия, и сертификат(ы) открытого ключа объекта (объектов), для которых запрашивается лицензия. Следует отметить, что объектом, запрашивающим лицензию, не обязательно должен быть объект, для которого запрашивается лицензия. Обычно лицензия включает в себя описание прав из ПМП 308, зашифрованный ключ, который может дешифровать зашифрованный контент, и цифровую подпись на описание прав и зашифрованный ключ для установления легальности и предотвращения злонамеренного изменения программных документов.

Предварительно клиентский API 306 направляет подписанную метку 308 прав контента 310 с управляемыми правами на сервер 320 УЦП по сети 330 связи. Как описано выше, метка 308 прав содержит ключ контента (СК), зашифрованный в соответствии с открытым ключом сервера 320 УЦП (PU-DRM) (т.е. (PU-DRM(CK))). Затем в процессе выдачи лицензии сервер 320 УЦП применяет (PR-DRM) к (PU-DRM(CK)) для получения (СК). Далее он использует открытый ключ (PU-ENTITY) в сертификате открытого ключа, который передается в запросе на лицензию, для повторного шифрования (СК) (т.е. (PU-

ENTITY(СК))). Вновь зашифрованный (PU-ENTITY(СК)) затем помещается в лицензию. Таким образом, лицензия может быть возвращена вызывающей стороне без опасности раскрытия (СК), так как только обладатель секретного ключа (PR-ENTITY), соответствующий (PU-ENTITY), может восстановить (СК) из (PU-ENTITY(СК)). Клиентский API 306 затем использует (СК) для дешифрования зашифрованного контента для формирования дешифрованного цифрового контента 312. Клиентское приложение 302 затем может использовать дешифрованный цифровой контент 312 согласно правам, которые предусмотрены в лицензии.

Альтернативно, и как подробно изложено ниже, клиент, такой как публикующий клиент, может, например, выдать лицензию на использование самому себе, чтобы потреблять контент.

Обратимся теперь к фиг.6А и 6В, где показан способ лицензирования цифрового контента с управляемыми правами. На этапе 602 выдающий лицензию объект, такой как сервер 320 УЦП, принимает запрос на лицензию, включающий в себя либо сертификат открытого ключа, либо идентификационные данные для каждого одного или нескольких запрашивающих лицензиатов. Предположительно, если заданы идентификационные данные, то сервер 320 УЦП может обеспечить соответствующий сертификат открытого ключа из каталога, базы данных и т.п. Если лицензия запрашивается только для одного лицензиата, то назначается только один сертификат или идентификатор. Если лицензия запрашивается для множества обладателей лицензиатов, то сертификат или идентификатор может быть назначен для каждого потенциального лицензиата. На этапе 604 выполняется аутентификация запрашивающего объекта (т.е. объекта, выполняющего запрос на лицензию), если это требуется. На этапе 606 определяется, разрешено ли этому объекту запрашивать лицензию снова, если это требуется.

Если на этапе 608 выдающий объект определяет, что сертификат открытого ключа не включен в запрос на лицензию, то выдающий объект использует заданные идентификационные данные для выполнения поиска соответствующего сертификата открытого ключа в службе каталогов или базе данных. Если на этапе 610 выдающий объект определяет, что сертификат находится в каталоге, то на этапе 612 сертификат извлекается. Если сертификат не может быть найден для данного потенциального лицензиата либо в запросе, либо в каталоге, то сервер лицензий не генерирует лицензию для этого потенциального лицензиата, и на этапе 614 запрашивающему объекту возвращается код ошибки.

Предполагая, что сервер 320 УЦП имеет сертификат открытого ключа по меньшей мере для одного потенциального лицензиата, на этапе 616 такой сервер 320 УЦП удостоверяется в том, что сертификат каждого лицензиата заслуживает доверия. Если сервер 320 УЦП удостоверяется в обратном, то сервер 320 УЦП определяет, что объект, выдавший сертификат лицензиату, не находится в списке доверенных объектов, выдающих сертификаты, тогда запрос завершается неуспешно для этого лицензиата, и на этапе 614 генерируется под ошибки. Таким образом, любой потенциальный лицензиат, сертификат которого не выдается доверенным выдавателем (выдающим объектом), не получит лицензию.

Кроме того, сервер 320 УЦП предпочтительно выполняет проверку подлинности цифровой подписи по всем элементам в цепочке сертификатов, идущей от сертификатов доверенного выдавателя до сертификатов открытого ключа индивидуальных лицензиатов. Процесс проверки подлинности цифровых подписей в цепочке представляет собой общеизвестный алгоритм. Если сертификат открытого ключа для заданного потенциального лицензиата не проходит проверку на подлинность, или не проходит проверку на подлинность сертификат в цепочке, то потенциальный лицензиат не является доверенным, и лицензия, поэтому, не выдается этому потенциальному лицензиату. В противном случае, на этапе 618 может быть выдана лицензия. Процесс повторяется на этапе 620 до тех пор, пока не будут обработаны все объекты, для которых была запрошена лицензия.

Как показано на фиг.6В, сервер 320 УЦП переходит к проверке подлинности подписанной метки 308 прав, которая принимается в запросе на лицензию. В одном варианте выполнения сервер 320 УЦП имеет оригинал каждой метки прав, подписанной им. Затем во время действия лицензии (на этапе 622) сервер 320 УЦП может извлечь копию оригинала метки прав. Оригинал метки прав может быть более новым, чем копия метки прав, посланная в запросе на лицензию, и, поэтому, будет меткой прав, используемой для получения запрашиваемой лицензии. Если не найден оригинал метки прав, то сервер 320 УЦП на этапе 624 определяет согласно предварительно определенной политике, выдавать ли лицензию, основанную на метке прав в запросе. Если политика не позволяет этого, то запрос на лицензию завершается неуспешно на этапе 626, и API 306 на этапе 628 возвращается код ошибки.

На этапе 630 сервер 320 УЦП проверяет подлинность ПМП 308 и, в частности, ее цифровую подпись. Если проверка подлинности ПМП 308 завершается неуспешно, то запрос на лицензию завершается неуспешно на этапе 626, и API 306 на этапе 628 возвращается код ошибки.

После завершения всех проверок подлинности сервер УЦП составляет лицензию для каждой подтвержденной лицензии на основе ПМП 308. На этапе 632 сервер 320 УЦП генерирует описание соответствующих прав для лицензии, подлежащей выдаче каждому лицензиату. Для каждого лицензиата сервер 320 УЦП оценивает идентификационные данные, указанные в сертификате открытого ключа этого обладателя лицензии, среди идентификационных данных, указанных в описании прав в метке прав. На этапе 636 сервер 320 УЦП получает (PU-DRM(K2)) и (K2(CK)) из ПМП 308 и применяет (PR-DRM) для получения (СК). Выдающий объект затем повторно шифрует (СК), используя (PU-ENTITY) из сертификата открытого ключа лицензиата, получая в результате (PU-ENTITY(CK)). На этапе 638 сервер 320 УЦП сцепляет сгенерированное описание прав с (PU-ENTITY(CK)) и цифровым образом подписывает результирующую структуру данных, используя (PR-DRM) (т.е. S(PR-DRM)). Подписанная структура данных, таким образом, является лицензией для этого конкретного лицензиата.

На этапе 640 сервер 320 УЦП определяет, что больше нет лицензий для генерирования по конкретному запросу. Сгенерированные лицензии затем возвращаются запрашивающему объекту на этапе 642 вместе с соответствующей цепочкой сертификатов, которая связывает лицензии с доверяемым органом.

Самопубликация подписанной метки 308 прав

В одном варианте выполнения настоящего изобретения ПМП 308 может быть подписана самим запрашивающим/публикующим пользователем. Следовательно, такому пользователю необязательно обращаться к серверу 320 УЦП для получения ПМП 308 для ассоциированной с ней порции контента. В результате самопубликация также может упоминаться как автономная публикация. В таком варианте выполнения публикующий пользователь также должен быть способен выдать самому себе лицензию издателя, особенно ввиду того, что самопубликуемый контент теперь защищен посредством УЦП, и такая лицензия издателя требуется для того, чтобы дать возможность публикующему пользователю воспроизвести защищенный контент. Также следует понимать, что публикующему пользователю может быть разрешено выдавать лицензии другим пользователям.

В частности, и ссылаясь теперь на фиг.7, в варианте выполнения автономно публикующему пользователю сначала предоставляется возможность автономной публикации посредством приема от сервера 320 УЦП сертификата 810 автономной публикации (АП, OLP), включающего открытый ключ (PU-OLP) и соответствующий секретный ключ (PR-OLP), зашифрованный согласно открытому ключу, прямо или косвенно доступному для доверяемого компонента 18 (фиг.11) пользователя (PU-ENTITY), получая в результате (PU-ENTITY(PR-CERT)). Следует отметить, что (PU-ENTITY) может быть, например, открытым ключом доверенного компонента 18 или может быть открытым ключом пользователя, который является доступным посредством открытого ключа доверенного

компонента 18. Сертификат 810 АП должен быть подписан секретным ключом сервера 320 УЦП (PR-DRM), так что такой сервер 320 УЦП может проверить такой сертификат АП, что подробно описывается ниже.

Кроме того, сертификат 810 АП должен включать в себя цепочку сертификатов от (PU-DRM), ведущую в обратном направлении к доверенному органу, которому доверяет доверенный компонент 18 публикующего пользователя или другого пользователя, так что такой доверенный компонент 18 может проверить такой сертификат 810 АП и любой другой сертификат или лицензию, которая связана с таким сертификатом 810 АП, что описывается ниже. Вкратце, и как это следует понимать, цепочка сертификатов начинается с корневого сертификата, подписанного секретным ключом доверенного органа и имеющего открытый ключ следующего сертификата в цепочке. Каждый промежуточный сертификат в цепочке затем подписывается секретным ключом, соответствующим открытому ключу предыдущего сертификата в цепочке, и имеет открытый ключ следующего сертификата в цепочке. Наконец, сертификат или лицензия, к которой присоединена цепочка, подписывается секретным ключом, соответствующим открытому ключу последнего сертификата в цепочке.

Таким образом, для того чтобы проверить сертификат или лицензию, к которой присоединена цепочка, получают информацию об открытом ключе, соответствующем секретному ключу доверенного органа, и такой открытый ключ доверенного органа используется для проверки подписи корневого сертификата в цепочке. Предполагая, что проверка подписи корневого сертификата завершилась успешно, открытый ключ из корневого сертификата получают и используют для проверки подписи первого промежуточного сертификата в цепочке. Процесс последовательно повторяется по цепочке до тех пор, пока не будет проверена каждая ее подпись, и тогда открытый ключ из последнего промежуточного сертификата в цепочке получают и используют для проверки подписи сертификата или лицензии, к которой присоединена цепочка.

Следует понимать, что сертификат 810 АП создает звено в цепочке доверия между контентом 304, который должен быть опубликован автономно, и сервером 320 УЦП, который будет выдавать лицензию на контент 304. Сертификат 810 АП может быть создан, основываясь на расширяемом языке разметки (XML)/расширяемом языке разметки прав (XrML) или любом другом подходящем языке.

Также следует понимать, что сертификат 810 АП и присоединенная цепочка сертификатов разрешают публикующему пользователю выполнить самопубликацию. Следует оценить тот факт, что пара ключей (PU-OLP, PR-OLP) отдельна от (PU-ENTITY, PR-ENTITY) и используется специально для самопубликации. Следует отметить, что можно обходиться без пары ключей (PU-OLP, PR-OLP), в этом случае сертификат 810 УЦП включает в себя только открытый ключ пользователя (PU-ENTITY) и подписывается секретным ключом сервера 320 УЦП (PR-DRM), так что такой сервер 320 УЦП может его проверить.

Самопубликация отличается от публикации, показанной на фиг.4, тем, что пользователь, по существу, замещает сервер 320 УЦП в отношении этапов, выполняемых им. Существенно то, что пользователь подписывает представленную метку прав, включающую в себя (PU-DRM(K2)) и (K2(rightsdata)) или включающую в себя (PU-DRM(CK)) и (CK(rightsdata)) (причем последний показан на фиг.7 и 8), с помощью (PR-OLP), полученного из сертификата 810 УЦП (т.е. S(PR-OLP)), получая в результате подписанную метку 308 прав (ПМП). Клиент доверенного компонента 18 при использовании сертификата 810 АП обычно проверяет его, основываясь на присоединенной цепочке сертификатов. Следует понимать, что доверенный компонент 18 пользователя получает (PR-OLP) из сертификата 810 АП посредством получения (PU-ENTITY(PR-OLP)) из такого сертификата 810 АП и применения к нему (PR-ENTITY). Следует, однако, отметить, что публикующий пользователь не может проверить то, может ли сервер 320 УЦП принудительно применять права в самопубликуемой ПМП 308. Следовательно, сервер 320 УЦП сам должен выполнить проверку в тот момент, когда запрашивается лицензия, основываясь на

самопубликуемой ПМП 308.

Если публикующий пользователь выполняет самопубликацию ПМП 308, то пользователь сцепляет такую самопубликуемую ПМП 308 и сертификат 810 АП, используемый для ее получения, с контентом 304, и такой контент 304 с ПМП 308 и сертификатом 810 УЦП распространяется как контент 310 с управляемыми правами другому пользователю. После этого другой пользователь запрашивает и получает лицензию на контент 304/310 от сервера 320 УЦП, по существу, способом, аналогичным способу по фиг.6А и 6В. В данном случае, однако, запрашивающий лицензию пользователь представляет серверу 320 УЦП как самопубликуемую ПМП 308, так и сертификат 810 АП, сцепленные с контентом 304. Затем сервер 320 УЦП проверяет S(PR-DRM) в сертификате 810 АП, основываясь на соответствующем (PU-DRM), и получает (PU-OLP) из сертификата 810 УЦП. Затем сервер 320 УЦП проверяет S(PR-OLP) в ПМП 308 на основе полученного (PU-CERT) и продолжает функционировать по-прежнему. Следует однако отметить, что так как публикующий пользователь не проверял, может ли сервер 320 УЦП принудительно применить права в ПМП 308, и, как было изложено выше, сервер 320 УЦП сам должен в этот момент выполнить проверку.

Следует также отметить, что серверу 320 УЦП необходимо только проверить S(PR-DRM) в сертификате 810 АП, так как, предположительно, он доверяет себе. Следовательно, связанная цепочка сертификатов от сертификата 810 АП необязательно должна быть послана на сервер 320 УЦП вместе с таким сертификатом 810 АП, если, конечно, цепочка не является необходимой иным образом, таким как, например, если сама цепочка является, по меньшей мере частично, базовым компонентом для S(PR-DRM).

Важно, впрочем, что публикующий пользователь может воспроизвести защищенный контент 304/310 без необходимости обращения к серверу 320 УЦП за лицензией. Другими словами, публикующий пользователь, который автономно публикует контент 304/310 без обращения к серверу 320 УЦП, основываясь на сертификате 810 АП, также может выдать самому себе лицензию автономным образом без обращения к серверу 320 УЦП, так что такой пользователь может воспроизводить автономно публикуемый контент 304/310. Следовательно, публикующий пользователь может продолжить работу с самоопубликованным контентом 310 без какой-либо необходимости соединения с сервером 320 УЦП.

Тогда в одном варианте выполнения настоящего изобретения и обращаясь теперь к фиг.8, публикующий пользователь выдает самому себе лицензию 820 автономного издателя, подписанную посредством (PR-OLP) на основе автономно опубликованной ПМП 308 и включающую в себя сертификат 810 АП и его цепочку сертификатов. Предположительно, лицензия 820 издателя предоставляет публикующему пользователю полный доступ к автономно опубликованному контенту 310, хотя также может быть предоставлен доступ в меньшем объеме. Лицензия 820 издателя может быть написана на языке XML/XrML или на другом языке, как в случае с другими лицензиями УЦП. Следует понимать, что лицензия 820 издателя включает в себя ключ контента (CK), зашифрованный согласно (PU-ENTITY), который может быть получен доверенным компонентом 18 вычислительного устройства 14 пользователя, образуя (PU-ENTITY(CK)).

Цепочка для лицензии 820 издателя, таким образом, идет от такой лицензии 820 к сертификату 810 АП, а затем обратно к корневому сертификату от доверенного органа, возможно посредством одного или нескольких промежуточных сертификатов. Так как доверенный компонент 18 пользователя, предположительно, может получить открытый ключ, соответствующий секретному ключу доверенного органа, который использовался для подписи корневого сертификата, то доверенный компонент 18 сам может проверить лицензию 820 издателя посредством ее цепочки сертификатов и после проверки затем может получить от него (PU-ENTITY(CK)), применить (PR-ENTITY) к нему для получения (CK) и применить (CK) к (CK(content)), получая в результате контент 304 с целью его воспроизведения. Как результат, публикующий пользователь может продолжить работу с контентом 310, автономно опубликованным им, в то же самое время оставаясь

автономным.

Тогда в соответствии с вышеописанным и обращаясь теперь к фиг.9, публикующий пользователь автономно публикует контент 304/310 и выдает самому себе лицензию 820 автономного издателя для такого контента 304/310 следующим способом.

Предварительно, и как это следует понимать, контент 304 разрабатывается соответствующим образом и шифруется согласно ключу (СК) контента (этап 901), и публикующий пользователь создает метку прав для контента 304 с соответствующей информацией {((PU-DRM)CK) и (CK(rightsdata)), например} (этап 903). После этого публикующий пользователь, который, предположительно, уже владеет сертификатом 810 АП от сервера 320 УЦП, получает такой сертификат 810 АП (этап 905) и проверяет его, основываясь на его подписи и цепочке сертификатов, которая ведет в обратном направлении к корневому органу (этап 907). Следует понимать, что такая проверка фактически выполняется доверенным компонентом 18 на вычислительном устройстве 14 публикующего пользователя. Допустим, что проверка успешна, тогда публикующий пользователь/доверенный компонент 18 (ниже «публикующий пользователь») извлекает (PU-ENTITY(PR-OLP)) из сертификата 810 АП (этап 909), применяет (PR-ENTITY) к (PU-ENTITY(PR-OLP)) для получения (PR-OLP) (этап 911) и затем подписывает созданную метку прав с таким (PR-OLP) для создания ПМП 308 (этап 913).

После этого публикующий пользователь сцепляет такую ПМП 308 и сертификат 810 АП, используемый для ее получения, с контентом 304 и формирует самопубликуемый контент 310 (этап 915), и, следовательно, такой контент 310 с управляемыми правами можно передать другому пользователю. Тем не менее, для того чтобы публикующий пользователь продолжал использовать или воспроизводить контент 310, такой публикующий пользователь должен выдать самому себе соответствующую лицензию 820 автономного издателя.

Таким образом, публикующий пользователь создает для себя лицензию 820 издателя посредством определения соответствующих данных о правах и шифрования их согласно ключу (СК) контента, получая в результате (CK(rightsdata)) (этап 917). Следует отметить при этом, что такие данные о правах могут быть получены на основе ПМП 308 из контента 310, могут быть некоторым набором данных о правах по умолчанию, предоставляющих публикующему пользователю частичный или полный доступ к самопубликуемому контенту 310, или могут быть получены из другого источника. Кроме того, публикующий пользователь шифрует ключ (СК) контента согласно (PU-ENTITY) для формирования (PU-ENTITY(CK)) (этап 919). Такой (CK(rightsdata)) и (PU-ENTITY(CK)) затем форматируются в лицензию 820 издателя (этап 921), к ней присоединяется сертификат 810 АП и его цепочка сертификатов (этап 923), и такая лицензия 820 издателя подписывается на основе (PR-OLP), который был получен на этапе 911 (этап 925). Следует отметить здесь, что контент 304 (т.е. (СК(content))), лицензия 820 на публикацию и сертификат АП в комбинации формируют цепочку 830 цифровых элементов, ведущую в обратном направлении к доверенному органу.

Далее, для того чтобы публикующий пользователь воспроизводил опубликованный контент 310, и обращаясь теперь к фиг.10, такому публикующему пользователю нет необходимости обращаться к серверу 320 УЦП, но вместо этого он получает открытый ключ, соответствующий секретному ключу доверенного органа, который использовался для подписи корневого сертификата (этап 1001), проверяет корневой сертификат (этап 1003) и затем проверяет каждый промежуточный сертификат в цепочке (этап 1005) посредством получения, для каждого такого промежуточного сертификата, открытого ключа из предыдущего сертификата и его использования для проверки подписи такого сертификата. После этого (PU-DRM) из последнего сертификата в цепочке используют для проверки подписи сертификата 810 АП (т.е. S(PR-DRM)) (этап 1007), (PU-OLP) получают из сертификата 810 АП (этап 1009), и такой (PU-OLP) используют для проверки лицензии 820 издателя (т.е. S(PR-OLP)) (этап 1010).

Если проверена лицензия 820 издателя, то из нее извлекают (CK(rightsdata)) и (PU-

ENTITY(CK)) (этап 1011), (PR-ENTITY) применяют к (PU-ENTITY(CK)), получая в результате (CK) (этап 1013), и (CK) применяют к (CK(rightsdata)), получая в результате данные о правах (этап 1015). Далее следует понимать, что данные о правах анализируются доверенным компонентом 18 вычислительного устройства 14 публикующего пользователя для определения того, что такие данные о правах разрешают воспроизведение желаемым образом (этап 1017), такой доверенный компонент 18, таким образом, применяет (CK) к (CK(content)) из контента 310, получая в результате контент (этап 1019), и такой контент затем направляется соответствующему воспроизводящему приложению для фактического воспроизведения (этап 1021). Таким образом, этапы по фиг.10, фактически, проходят цепочку 830 цифровых элементов от доверенного органа до контента 304.

Следует отметить, что доверенный компонент 18 может, предположительно, применить (CK) к (CK(content)), получая в результате контент без первоначального анализа данных о правах и независимо от того, что данные о правах могут разрешать или запрещать, но он является доверенным и сконфигурирован так, чтобы фактически формировать контент только после анализа данных о правах и удовлетворения собственному требованию, что данные о правах разрешают воспроизведение такого контента. Опять же, в результате обладания лицензией 820 издателя публикующий пользователь может продолжать работать с контентом 310, автономно им опубликованным, в то же самое время оставаясь автономным в плане того, что нет необходимости обращаться к серверу 320 УЦП.

Регистрация и субрегистрация серверов УЦП

В архитектуре, показанной на фиг.3, изображен только один сервер 320 УЦП. Однако следует понимать, что такая архитектура может и, скорее всего, действительно включает в себя множество серверов 320 УЦП. В частности, и в одном варианте выполнения настоящего изобретения, такая архитектура включает в себя распределенную сеть серверов 320 УЦП. Каждый из таких серверов 320 УЦП может иметь любую конкретную функцию, и все серверы 320 УЦП могут быть организованы любым подходящим образом в пределах сущности и объема настоящего изобретения.

Например, и обращаясь теперь к фиг.12, конкретная организация может иметь один или несколько серверов 320 УЦП уровня пользователя для целей подписания меток прав с целью получения ПМП 308, выдачи лицензий 16, предоставления лицензий 320 на публикацию, выдачи сертификатов пользователям, выдачи сертификатов вычислительным устройствам 14 и т.д. Каждый такой сервер 320 УЦП уровня пользователя, например, может быть назначен по географическому принципу или может быть назначен, основываясь на функции или загрузке. Аналогично, чтобы осуществлять надзор за многочисленными серверами 320 УЦП пользовательского уровня, организация может иметь один или несколько управляющих серверов 320 УЦП. Такие основанные на организации сервера 320 УЦП могут быть расположены за средством сетевой защиты организации, если это потребуется.

В дополнение к основанным на организации серверам 320 УЦП также могут быть межорганизационные серверы 320 УЦП, которые обеспечивают функциональные возможности УЦП объединения организаций. Например, такие межорганизационные серверы 320 УЦП могут разрешать двум организациям совместно использовать некоторый контент 12 УЦП. Также, может быть сеть серверов-контролеров 320 УЦП, которые активируют все другие серверы 320 УЦП. Например, такие серверы-контролеры 320 УЦП могут осуществлять надзор и обслуживать все другие серверы 320 УЦП и обеспечивать соответствующее связывание для всех других серверов 320 УЦП с корневым или доверенным органом, который является базовым компонентом для цепочки сертификатов, описанной ранее. Такие не основанные на организации серверы 320 УЦП, вероятно, не расположены за каким-либо средством сетевой защиты организации.

Существенно, что каждый сервер 320 УЦП в архитектуре по фиг.12 должен быть способен доказать, что ему следует доверять. Таким образом, как следует из вышеописанного описания цепочки сертификатов, каждый сервер 320 УЦП при входе в эту

архитектуру обеспечивается сертификатом 1310 регистрации, как показано на фиг.13. Существенно, и в одном варианте выполнения настоящего изобретения, что сертификат 1310 регистрации предоставляется входящему серверу 320 УЦП (ниже «сервер 320 УЦП-В») посредством другого «регистрирующего» сервера 320 УЦП, который уже находится в архитектуре (ниже «сервер 320 УЦП-Р»). Также существенно, что к предоставленному сертификату 1310 регистрации от регистрирующего сервера 320 УЦП-Р присоединена цепочка сертификатов 1320, включающая в себя сертификат 1310 регистрации регистрирующего сервера 320 УЦП, сертификат 1310 регистрации сервера 320 УЦП, который зарегистрировал регистрирующий сервер 320 УЦП-Р, и т.д. по всему пути в обратном направлении к корневому серверу 320 УЦП. Такой корневой сервер 320 УЦП может представлять корневой или доверенный орган, либо цепочка сертификатов 1320 может продолжаться далее и достигать корневого или доверенного органа. Теперь следует принять во внимание, что такой сертификат 1310 регистрации и цепочка сертификатов 1320 в комбинации образуют цепочку сертификатов, которая присоединяется к сертификату 810 АП, предоставленному зарегистрированным или вошедшим сервером 320 УЦП-В публикующему пользователю, такой как пользователь по фиг.8.

В одном варианте выполнения настоящего изобретения сертификат 1310 регистрации, предоставленный серверу 320 УЦП-В посредством сервера 320 УЦП-Р, выполнен в форме, аналогичной сертификату, основанному на XrML 1.2. Следует понимать, что такой тип сертификата 1310 не представляется независимо какой-то третьей стороной, и, таким образом, такой тип сертификата 1310 не представляет собой какой-либо вид независимого поручительства третьей стороны в отношении обладателя такого сертификата 1310.

В одном варианте выполнения настоящего изобретения способ, с помощью которого конкретный сервер 320 УЦП-В регистрируется в архитектуре, зависит от того, знает ли регистрирующий сервер 320 УЦП-Р или имеет причину доверять входящему серверу 320 УЦП-В. Если это не так, то серверу 320 УЦП-В потребуется доказать серверу 320 УЦП-Р, что он заслуживает доверия и будет принудительно применять архитектуру УЦП. Если же это так, то серверу 320 УЦП-В не нужно будет доказывать серверу 320 УЦП-Р, что он заслуживает доверия, по меньшей мере, не в такой степени. Таким образом, недоверяющий/незнающий сервер 320 УЦП «регистрирует» сервер 320 УЦП-В, тогда как знающий/доверяющий сервер 320 УЦП-Р «субрегистрирует» сервер 320 УЦП-В.

Обычно сервер 320 УЦП-Р знает/доверяет серверу 320 УЦП-В, если оба эксплуатируются в одной организации или для нее, хотя знание/доверие также может возникнуть в результате других ситуаций в пределах сущности и объема настоящего изобретения. Таким образом, способ, с помощью которого конкретный сервер 320 УЦП-В регистрируется в архитектуре, обычно зависит от того, основан или не основан на организации регистрирующий сервер 320 УЦП-Р. В результате, не основанный на организации сервер 320 УЦП-Р «регистрирует» сервер 320 УЦП-В, тогда как основанный на организации сервер 320 УЦП-Р «субрегистрирует» сервер 320 УЦП-В.

Регистрация

В одном варианте выполнения настоящего изобретения, и обращаясь теперь к фиг.14, незнающий/недоверяющий сервер 320 УЦП-Р регистрирует сервер 320 УЦП-В следующим образом.

Предварительно, следует понимать, что сервер 320 УЦП-В, желающий зарегистрироваться у незнающего/недоверяющего сервера 320 УЦП-Р, скорее всего, неизвестен такому серверу 320 УЦП-Р. Следовательно, и в одном варианте выполнения настоящего изобретения, сервер 320 УЦП-В должен обеспечить сертификат 1330 поручительства от третьей стороны, желающей поручиться за такой сервер 320 УЦП-В (этап 1401). Обычно такой третьей стороной является независимый выдающий сертификат агент, которому доверяет сервер 320 УЦП-Р для выполнения такого поручительства, такой как, например, корпорация VERISIGN из г. Маунтин-Вью, шт. Калифорния. Такой сертификат 1330 поручительства может быть, например, в форме, аналогичной сертификату стандарта X.509. Следует отметить, что для сервера 320 УЦП-Р,

полагающегося на доверенную третью сторону в отношении поручительства за сервер 320 УЦП-В, уменьшается ответственность такого сервера 320 УЦП-Р за любые неправильные действия сервера 320 УЦП-В.

Как следует понимать и что является типичным, и что также показано на фиг.13, сертификат 1330 поручительства включает в себя открытый ключ (PU-V) и соответствующий секретный ключ (PR-V), подписывается доверенной третьей стороной и может сопровождаться цепочкой сертификатов, ведущей к известному корню с целью проверки подлинности. Что также является типичным, (PR-V) в сертификате 1330 поручительства защищается таким образом, что является доступным для сервера 320 УЦП-В, в отношении которого представлено поручительство, что является основным для сертификата 1330 поручительства. Например, и как показано на фиг.13, (PR-V) может быть зашифрован согласно соответствующему открытому ключу.

В архитектуре УЦП входящий сервер 320 УЦП-В должен иметь уникальные идентификационные данные. Здесь следует понимать, что идентификационные данные УЦП, скорее всего, отличаются от (PU-V, PR-V), хотя идентификационные данные УЦП также могут совпадать с такими (PU-V, PR-V) в пределах сущности и объема настоящего изобретения. Следовательно, для задания таких идентификационных данных такой сервер 320 УЦП-В генерирует или получает новую пару из открытого/секретного ключей (PU-E, PR-E) (этап 1403). Также, в архитектуре УЦП регистрирующий сервер 320 УЦП-В должен принять решение в отношении того, какие объекты могут аннулировать его полномочия на участие. Следовательно, такой сервер 320 УЦП-В идентифицирует каждый такой объект с полномочиями аннулирования в списке, возможно, посредством его открытого ключа (этап 1405). Сервер 320 УЦП-В должен быть способен доказать регистрирующему серверу 320 УЦП-Р, что этот сервер УЦП-В действительно обладает сертификатом 1330 поручительства, который был получен на этапе 1401. Следовательно, сервер 320 УЦП-В либо использует (PR-V) из сертификата 1330 поручительства для шифрования (PU-E), получая в результате (PR-V(PU-E)) в качестве признаков обладания, либо подписывает (PU-E) с помощью (PR-V), получая в результате (PU-E)S(PR-V) в качестве признаков обладания (этап 1407). В любом случае применение (PU-V) для дешифрования (PU-E) или проверки подписи устанавливает факт обладания (PR-V) и, следовательно, сертификатом 1330 поручительства.

Сервер 320 УЦП-В имеет сертификат 1330 поручительства, (PU-E) и (PR-E), список объектов с полномочиями аннулирования и (PR-V(PU-E)) или (PU-E)S(PR-V) в качестве признаков обладания. Для того чтобы запросить затем регистрацию, такой сервер 320 УЦП-В посылает на сервер 320 УЦП-Р сертификат 1330 поручительства, (PU-E), список объектов с полномочиями аннулирования и (PR-V(PU-E)) или (PU-E)S(PR-V) в качестве признаков обладания (этап 1409), и сервер 320 УЦП-Р переходит к регистрации этого запрашивающего сервера 320 УЦП-В. Следует отметить, что запрос или его часть может быть в виде сертификата, подписанного посредством (PR-E).

В частности, сервер 320 УЦП-Р проверяет подлинность сертификата 1330 поручительства, основываясь на его подписи, посредством доверенной третьей стороны и цепочки сертификатов, ведущей к известному корню (этап 1411). Таким образом, сервер 320 УЦП-Р удостоверяется в том, что в отношении сервера 320 УЦП-В представлено поручительство. Также, сервер 320 УЦП-Р проверяет признаки обладания посредством применения (PU-V) из запроса либо для дешифрования (PU-E), либо проверки подписи и, таким образом устанавливает факт обладания (PR-V) и, следовательно, сертификатом 1330 поручительства в запросе (этап 1410). В дополнение к сказанному, существенно, что сервер 320 УЦП-Р выполняет любые специальные логические операции, необходимые для принятия решения о том, удовлетворить ли запрос (этап 1413). Такие специальные логические операции могут представлять собой любые соответствующие логические операции в пределах сущности и объема настоящего изобретения, и могут, например, включать в себя фоновую проверку сервера 320 УЦП-В и/или его оператора, определение того, имеет ли сервер 320 УЦП-В текущий доверенный компонент 18 и/или операционную

систему или т.п., определение того, находится ли сервер 320 УЦП-В в списке аннулирования или в другом списке, за которым ведется наблюдение, и т.п.

Предположив, что специальные логические операции позволяют удовлетворить запрос, тогда, согласно одному варианту выполнения настоящего изобретения, сервер 320 УЦП-Р генерирует сертификат 1310 регистрации для сервера 320 УЦП-В (этап 1415). В частности, и как показано на фиг.13, сервер 320 УЦП-Р включает в сертификат 1310 регистрации:

- идентификатор сервера 320 УЦП-Р, такой как его открытый ключ (PU-R);
- идентификатор сервера 320 УЦП-В, такой как (PU-E);
- идентифицирующие признаки из сертификата 1330 поручительства, включающие в себя доверенную третью сторону, которая выдала его, серийный номер из сертификата 1330 поручительства и выдавателя, идентифицированного в сертификате 1330 поручительства;
- любую информацию об интервале подлинности, задающую интервал, в течение которого сертификат 1310 регистрации является подлинным, такой как, например, интервал дат;
- список объектов с полномочиями аннулирования;
- подпись, основанную на секретном ключе сервера 320 УЦП-Р (PR-R), соответствующем (PU-R);
- и любую другую соответствующую информацию.

Такая другая соответствующая информация может включать в себя, но не в ограничительном смысле: время, когда сертификат был выдан; индикацию того, какой вид деятельности, относящейся к УЦП, регистрируемому серверу разрешено выполнять, как например, всю деятельность, только активацию учетных записей, только подписание меток прав, только выдача лицензий на контент и комбинации вышеперечисленного; и допустимый временной интервал для выполнения деятельности, относящейся к УЦП. Следует отметить, что допустимый временной интервал отличается от интервала подлинности тем, что текущее время должно лежать в интервале подлинности, чтобы принять на обработку любой сертификат, который включает в себя сертификат 1310 регистрации в цепочке сертификатов. В противоположность этому, время выдачи дочерних сертификатов должно попадать в допустимый временной интервал родительского сертификата для выполнения деятельности, относящейся к УЦП. Следует понимать, что при генерировании сертификата 1310 регистрации сервер 320 УЦП-Р может первоначально генерировать информацию о сертификатах, а затем разрешать специальным логическим операциям генерировать дополнительную информацию или модифицировать существующую информацию. Такие специальные логические операции могут, например, обеспечивать то, что сервер 320 УЦП-Р включает в себя соответствующую информацию, или может принудительно применять предварительно определенную политику архитектуры УЦП. Конечно, подпись сертификата 1310 регистрации создается после выполнения любой такой специальной логической операции. Также следует понимать, что сервер 320 УЦП-Р присоединяет цепочку сертификатов 1320, которая ведет в обратном направлении к доверенному корневому органу к сгенерированному сертификату 1310 регистрации, так что сгенерированный сертификат 1310 регистрации может быть проверен на подлинность на основе такой цепочки сертификатов 1320.

Следует отметить, в частности, что идентифицирующие признаки из сертификата 1330 поручительства, находящиеся в сертификате 1310 регистрации, будут всегда перемещаться с таким сертификатом 1310 регистрации и служить в качестве моста к сертификату 1330 поручительства. Таким образом, такие идентифицирующие признаки показывают внешнему миру, что сервер 320 УЦП-Р полагается на выдавателя сертификата 1330 поручительства, представляющего доверенную третью сторону, для поручительства за сервер 320 УЦП-В, и уменьшается ответственность такого сервера 320 УЦП-Р за любые неправильные действия сервера 320 УЦП-В. Если сервер 320 УЦП-Р успешно сгенерировал сертификат 1310 регистрации с присоединенной цепочкой сертификатов

1320, то сервер 320 УЦП-Р затем возвращает его на запрашивающий сервер 320 УЦП-В (этап 1417), и вновь зарегистрированный сервер 320 УЦП-В хранит его в соответствующем месте для будущего использования (этап 1419). Как упоминалось выше, (PU-E) в сертификате 1310 регистрации и соответствующий (PR-E) представляют собой пару из открытого/секретного ключей, которые сервер 320 УЦП-В будет использовать в качестве (PU-DRM) и (PR-DRM) при подписании метки прав для получения ПМП 308, при выдаче сертификата 810 АП и при участии иным образом в архитектуре УЦП. Следовательно, такой сертификат 1310 регистрации и цепочка сертификатов 1320 в комбинации образуют цепочку сертификатов, которая присоединяется к такому сертификату 810 АП и ему подобным.

Субрегистрация

В одном варианте выполнения настоящего изобретения, и обращаясь теперь к фиг.15, знающий/доверяющий сервер 320 УЦП-Р субрегистрирует сервер 320 УЦП-В следующим образом.

Предварительно, необходимо принять во внимание, что серверу 320 УЦП-В, собирающемуся выполнить субрегистрацию посредством знающего/доверяющего сервера 320 УЦП-Р, необходимо все же идентифицировать себя такому серверу 320 УЦП-Р ввиду того, что такое знание или доверие не может быть полным. Однако такое требование идентификации не должно подниматься до уровня представления доверенной третьей стороной ввиду того, что серверу 320 УЦП-Р не хватает лишь небольшой части знания/доверия в отношении сервера УЦП-В. Следовательно, и в одном варианте выполнения настоящего изобретения, сервер 320 УЦП-В получает или обеспечивается некоторого рода мандатом 1340 (фиг.13), который может быть опознан сервером 320 УЦП-Р и подлинность которого, как ожидается, будет подтверждена им, и который идентифицирует сервер 320 УЦП-В для удовлетворения требований сервера 320 УЦП-Р (этап 1501).

Если оба сервера 320 УЦП-Р и УЦП-В находятся в одной и той же организации, то таким мандатом 1340 может быть основанный на организации мандат, такой как, например, идентификатор сети, если оба сервера 320 находятся в общей сети, идентификатор домена, если оба сервера 320 совместно используют общий домен, и т.д. Если оба сервера 320 УЦП-Р и УЦП-В не находятся в одной и той же организации, то таким мандатом 1340 все же может быть идентификатор сети, если оба сервера 320 находятся в общей сети, идентификатор домена, если оба сервера 320 совместно используют общий домен, и т.п., или может быть другим мандатом, таким как, например, мандат, выданный третьей стороной и опознаваемый сервером 320 УЦП-Р.

Следует отметить, что в настоящей ситуации сервер 320 УЦП-Р не полагается на то, что доверенная третья сторона поручается за сервер 320 УЦП-В, и, поэтому не уменьшается ответственность такого сервера 320 УЦП-Р за любые неправильные действия сервера 320 УЦП-В. Тем не менее, сервер 320 УЦП-Р собирается пойти на такой риск, основываясь на знании или доверии в отношении того, что сервер 320 УЦП-В, на самом деле, не выполнит такие неправильные действия. Как и раньше, в архитектуре УЦП входящий сервер 320 УЦП-В должен иметь уникальные идентифицированные данные. В данном случае следует понимать, что идентификационные данные УЦП, скорее всего, находятся отдельно от мандата 1340, хотя идентификационные данные УЦП также могут совпадать с мандатом 1340 в пределах сущности и объема настоящего изобретения. Следовательно, чтобы установить такие идентификационные данные, такой сервер 320 УЦП-В генерирует или получает новую пару из открытого/секретного ключей (PU-E, PR-E) (этап 1503). Как и раньше, в архитектуре УЦП субрегистрирующий сервер 320 УЦП-В должен принять решение в отношении того, какие объекты могут аннулировать его полномочия на участие. Следовательно, такой сервер 320 УЦП-В идентифицирует такой объект с полномочиями аннулирования в списке, возможно посредством его открытого ключа (этап 1505).

Сервер 320 УЦП-В имеет мандат 1340, (PU-E) и (PR-E), и список объектов с

полномочиями аннулирования. Для того чтобы затем запросить субрегистрацию, такой сервер 320 УЦП-В посылает мандат 1340, (PU-E), и список объектов с полномочиями аннулирования на сервер 320 УЦП-Р (этап 1507), и сервер 320 УЦП-Р переходит к субрегистрации такого запрашивающего сервера 320 УЦП-В. Следует отметить, что, как и раньше, запрос или его часть может быть в виде сертификата, подписанного посредством (PR-E).

В частности, сервер 320 УЦП-Р проверяет подлинность мандата 1340, основываясь на том, какие логические операции или ресурсы необходимы и доступны, чтобы таким образом проверить подлинность (этап 1509). Таким образом, сервер 320 УЦП-Р устанавливает, основываясь на проверенном мандате 1340, что серверу 320 УЦП-В следует доверять в отношении его готовности соблюдать и подчиняться архитектуре УЦП. Кроме того, и в соответствии с вышесказанным, сервер 320 УЦП-Р выполняет любые специальные логические операции, необходимые для принятия решения в отношении того, удовлетворить ли запрос (этап 1511).

Предположив, что специальные логические операции позволяют удовлетворить запрос, то тогда, согласно одному варианту выполнения настоящего изобретения, сервер 320 УЦП-Р генерирует сертификат 1310 субрегистрации для сервера 320 УЦП-В (этап 1513). В частности, и как показано на фиг.13, сервер 320 УЦП-Р включает в сертификат 1310 субрегистрации:

- идентификатор сервера 320 УЦП-Р, такой как его открытый ключ (PU-R);
- идентификатор сервера 320 УЦП-В, такой как (PU-E);
- мандат 1340 или ссылку на него;
- любую информацию об интервале подлинности, задающую интервал, в течение которого сертификат 1310 субрегистрации является подлинным, такой как, например, интервал дат;
- список объектов с полномочиями аннулирования;
- подпись, основанную на секретном ключе сервера 320 УЦП-Р (PR-R), соответствующем (PU-R);
- и любую другую соответствующую информацию.

Как и раньше, при генерировании сертификата 1310 субрегистрации сервер 320 УЦП-Р может первоначально генерировать информацию о сертификате и затем разрешает специальным логическим операциям генерировать дополнительную информацию или модифицировать существующую информацию. Также, подпись сертификата 1310 субрегистрации создается после выполнения любых таких специальных логических операций. Как и раньше, сервер 320 УЦП-Р присоединяет цепочку сертификатов 1320, которая ведет в обратном направлении к доверенному корневому органу к сгенерированному сертификату 1310 субрегистрации, так что подлинность сгенерированного сертификата 1310 субрегистрации может быть проверена на основе такой цепочки сертификатов 1320.

Следует отметить здесь, что мандат 1340 или ссылка на него, как считается, не является особенно необходимым, но может, тем не менее, быть включен для завершенности. Следует также отметить, что сертификат 1310 субрегистрации не содержит идентифицирующих признаков из сертификата 1330 поручительства ввиду того, что сертификат поручительства не требовался в настоящем сценарии субрегистрации.

Если сервер 320 УЦП-Р успешно сгенерировал сертификат 1310 субрегистрации с присоединенной цепочкой сертификатов 1320, то сервер 320 УЦП-Р затем возвращает его на запрашивающий сервер 320 УЦП-В (этап 1515), и прошедший субрегистрацию сервер 320 УЦП-В сохраняет его в соответствующем месте для будущего использования (этап 1517). Как и раньше, (PU-E) в сертификате 1310 субрегистрации и соответствующий (PR-E) представляют собой пару из отрытого/секретного ключей, которые сервер 320 УЦП-В будет использовать в качестве (PU-DRM) и (PR-DRM) при подписании метки прав для получения ПМП 308, при выдаче сертификата 810 АП и при участии иным образом в архитектуре УЦП. Следовательно, такой сертификат 1310 субрегистрации и цепочка

сертификатов 1320 в комбинации образуют цепочку сертификатов, которая присоединяется к такому сертификату 810 АП и ему подобным.

Заключение

Программирование, необходимое для осуществления процессов, выполняемых в связи с настоящим изобретением, является относительно простым и должно быть очевидным для специалистов в соответствующей области программирования. Следовательно, описание такого программирования не прилагается к этому документу. Далее, любое конкретное программирование может быть использовано для выполнения настоящего изобретения в пределах его сущности и объема.

В настоящем изобретении архитектура и способ принудительного применения и управления цифровыми правами (УЦП) позволяют производить контролируемое воспроизведение или проигрывание цифрового контента произвольного вида, где такой контроль является гибким и определяемым владельцем/разработчиком такого цифрового контента. Архитектура разрешает и способствует такому контролируемому воспроизведению, особенно в среде офиса или организации и т.п., где документы должны совместно использоваться среди определенной группы лиц или классов лиц. Такая архитектура включает в себя механизм для регистрации/субрегистрации предоставляющих санкции серверов 320 УЦП в архитектуре.

Следует понимать, что изменения могут быть сделаны в вариантах выполнения, описанных выше, в пределах соответствующих им концепций изобретения. Например, если лицензия или метка прав подписывается на основе данных о правах в ней, то такие данные о правах необязательно должны быть зашифрованы. Аналогично, при запросе и составлении сертификата 1310 регистрации или субрегистрации необязательно должен быть использован список объектов с полномочиями аннулирования и другая аналогичная информация. Следует понимать, поэтому, что настоящее изобретение не ограничивается описанными конкретными вариантами выполнения, но подразумевается, что оно охватывает модификации в пределах сущности и объема настоящего изобретения, определенного в прилагаемой формуле изобретения.

Формула изобретения

1. Способ регистрации входящего сервера управления цифровыми правами (УЦП-В) в системе управления цифровыми правами (УЦП), имеющей множество серверов УЦП, выполняющих функциональные возможности УЦП, посредством регистрирующего сервера управления цифровыми правами (УЦП-Р), так что входящий сервер УЦП-В должен быть доверенными в системе, содержащий этапы, на которых сервер УЦП-В обеспечивает пару из открытого/секретного ключей (PU-E, PR-E) для идентификации такого сервера УЦП-В в системе УЦП;

сервер УЦП-В обеспечивает представляющие его идентификационные данные;

сервер УЦП-В посылает запрос на регистрацию на сервер УЦП-Р, причем запрос включает в себя представляющие идентификационные данные и (PU-E);

сервер УЦП-Р проверяет подлинность представляющих идентификационных данных;

сервер УЦП-Р, если запрос должен быть удовлетворен, генерирует цифровой сертификат регистрации для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП, причем сгенерированный сертификат регистрации основан, по меньшей мере частично, на (PU-E); сервер УЦП-Р возвращает сгенерированный сертификат регистрации на запрашивающий сервер УЦП-В; и вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации в соответствующем месте для будущего использования, причем сервер УЦП-В с сертификатом регистрации может использовать его для выдачи документов с УЦП в системе УЦП.

2. Способ по п.1, в котором сервер УЦП-Р не имеет действительных оснований для доверия серверу УЦП-В, при этом способ содержит этапы, на которых сервер УЦП-В обеспечивает представляющие его идентификационные данные, содержащие сертификат поручительства от стороны, желающей поручиться за такой сервер УЦП-В, причем

сертификат поручительства включает в себя открытый ключ (PU-V) и соответствующий секретный ключ (PR-V); сервер УЦП-В использует (PU-E) и (PR-V) для формулирования признаков обладания, чтобы показать, что сервер УЦП-В обладает сертификатом поручительства; сервер УЦП-В посылает запрос на регистрацию на сервер УЦП-Р, причем запрос включает в себя сертификат поручительства, (PU-E) и признаки обладания; сервер УЦП-Р проверяет подлинность сертификата поручительства; сервер УЦП-Р проверяет признаки обладания; и сервер УЦП-Р, если запрос должен быть удовлетворен, генерирует цифровой сертификат регистрации для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП, причем сгенерированный сертификат регистрации основан, по меньшей мере частично, на сертификате поручительства и (PU-E).

3. Способ по п.2, содержащий этап, на котором сервер УЦП-В обеспечивает сертификат поручительства от независимого выдающего сертификат агента, который является доверенным для сервера УЦП-Р и на который полагается сервер УЦП-Р в отношении выполнения такого поручительства.

4. Способ по п.2, содержащий этап, на котором сервер УЦП-В обеспечивает сертификат поручительства по стандарту X.509.

5. Способ по п.2, содержащий этапы, на которых сервер УЦП-В обеспечивает сертификат поручительства, подписанный поручающейся стороной и сопровождаемый цепочкой сертификатов, ведущей к известному корню, для целей проверки подлинности; и сервер УЦП-Р проверяет подлинность сертификата поручительства на основе его подписи поручающейся стороной и цепочки сертификатов, чтобы удостовериться в том, что за сервер УЦП-В внесено поручительство.

6. Способ по п.2, содержащий этапы, на которых сервер УЦП-В выполняет одну из следующих операций: использование (PR-V) для шифрования (PU-E), получая в результате (PR-V(PU-E)) в качестве признаков обладания, или подписание (PU-E) с помощью (PR-V), получая в результате (PU-E)S(PR-V) в качестве признаков обладания; и

сервер УЦП-Р проверяет признаки обладания посредством применения (PU-V) из запроса для дешифрования (PU-E) или проверки подписи, чтобы удостовериться в том, что сервер УЦП-В владеет (PR-V) и, следовательно, сертификатом поручительства.

7. Способ по п.2, содержащий этапы, на которых сервер УЦП-Р генерирует сертификат регистрации, включающий в себя (PU-E) в качестве идентификатора сервера УЦП-В, идентифицирующие признаки для идентификации сертификата поручительства, и подпись, основанную на секретном ключе сервера УЦП-Р, причем идентифицирующие признаки для сертификата поручительства в сертификате регистрации служат в качестве моста к сертификату поручительства и показывают, что сервер УЦП-Р доверяет и полагается на поручающуюся сторону в отношении поручительства за сервер УЦП-В.

8. Способ по п.7, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя открытый ключ сервера УЦП-Р в качестве его идентификатора.

9. Способ по п.7. содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя информацию об интервале подлинности, задающую интервал, в течение которого сертификат регистрации является подлинным.

10. Способ по п.1, в котором сервер УЦП-Р имеет действительные основания для доверия серверу УЦП-В, при этом способ содержит этапы, на которых сервер УЦП-В обеспечивает представляющие его идентификационные данные, содержащие мандат, который может быть опознан сервером УЦП-Р и подлинность которого, как ожидается, будет подтверждена сервером УЦП-Р; сервер УЦП-В посылает запрос на регистрацию на сервер УЦП-Р, причем запрос включает в себя мандат и (PU-E); сервер УЦП-Р проверяет подлинность мандата; и сервер УЦП-Р, если запрос должен быть удовлетворен, генерирует цифровой сертификат регистрации для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП, причем сгенерированный сертификат регистрации основан, по меньшей мере частично, на мандате и (PU-E).

11. Способ по п.10, содержащий этап, на котором сервер УЦП-В обеспечивает мандат, выбранный из группы, состоящей из идентификатора сети или идентификатора домена и мандата, выданного третьей стороной.

12. Способ по п.10, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он включал в себя (PU-E) в качестве идентификатора сервера УЦП-В, идентифицирующие признаки для идентификации мандата и подпись, основанную на секретном ключе сервера УЦП-Р.

13. Способ по п.12, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя открытый ключ сервера УЦП-Р в качестве его идентификатора.

14. Способ по п.12, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя информацию об интервале подлинности, задающую интервал, в течение которого сертификат регистрации является подлинным.

15. Способ по п.1, дополнительно содержащий этап, на котором сервер УЦП-Р принимает решение в отношении того, удовлетворить ли запрос.

16. Способ по п.15, содержащий этап, на котором сервер УЦП-Р выполняет операции, выбранные из группы, состоящей из выполнения фоновой проверки сервера УЦП-В и/или его оператора, определения того, является ли текущим сервер УЦП-В и/или его часть, определения того, находится ли сервер УЦП-В в списке аннулирования или в списке, за которым ведется наблюдение, и комбинаций вышеперечисленного.

17. Способ по п.1, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он включал в себя (PU-E) в качестве идентификатора сервера УЦП-В и подпись, основанную на секретном ключе сервера УЦП-Р.

18. Способ по п.17, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя открытый ключ сервера УЦП-Р в качестве его идентификатора.

19. Способ по п.17, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя информацию об интервале подлинности, задающую интервал, в течение которого сертификат регистрации является подлинным.

20. Способ по п.17, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя идентифицирующие признаки для идентификации представляющих идентификационных данных.

21. Способ по п.1, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации посредством использования операций для генерирования по меньшей мере части информации в сертификате регистрации.

22. Способ по п.1, дополнительно содержащий этап, на котором сервер УЦП-Р присоединяет к сгенерированному сертификату регистрации цепочку сертификатов, которая ведет в обратном направлении к доверенному корневому органу, так что подлинность сгенерированного сертификата регистрации может быть проверена на основе такой цепочки сертификатов.

23. Способ по п.1, дополнительно содержащий этап, на котором сервер УЦП-В идентифицирует в списке объектов с полномочиями аннулирования по меньшей мере один объект с полномочиями аннулирования регистрации такого сервера УЦП-В в системе УЦП, содержащий этап, на котором сервер УЦП-В посылает запрос регистрации на сервер УЦП-Р, причем запрос включает в себя представляющие идентификационные данные, (PU-E) и список объектов с полномочиями аннулирования, и содержащий этап, на котором сервер УЦП-Р, если запрос должен быть удовлетворен, генерирует цифровой сертификат регистрации для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП, причем сгенерированный сертификат регистрации основан, по меньшей мере частично, на (PU-E) и списке объектов с полномочиями аннулирования.

24. Способ по п.23, содержащий этап, на котором сервер УЦП-В идентифицирует

каждый объект в списке объектов с полномочиями аннулирования посредством его открытого ключа.

25. Способ по п.23, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он включал в себя (PU-E) в качестве идентификатора сервера УЦП-В, список объектов с полномочиями аннулирования из запроса и подпись, основанную на секретном ключе сервера УЦП-Р.

26. Способ по п.1, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации в соответствии с XrML.

27. Способ регистрации входящего сервера управления цифровыми правами (УЦП-В) в системе управления цифровыми правами (УЦП), имеющей множество серверов УЦП, выполняющих функциональные возможности УЦП, посредством регистрирующего сервера управления цифровыми правами (УЦП-Р), так что входящий сервер УЦП-В должен быть доверенным в системе, содержащий этапы, на которых сервер УЦП-В обеспечивает пару из открытого/секретного ключей (PU-E, PR-E) для идентификации такого сервера УЦП-В в системе УЦП; сервер УЦП-В обеспечивает представляющие его идентификационные данные; сервер УЦП-В посылает запрос на регистрацию на сервер УЦП-Р, причем запрос включает в себя представляющие идентификационные данные и (PU-E), сервер УЦП-Р проверяет подлинность представляющих идентификационных данных и, если запрос должен быть принят на обработку, генерирует цифровой сертификат регистрации для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП, причем сгенерированный сертификат регистрации основан, по меньшей мере частично, на (PU-E), и возвращает сгенерированный сертификат регистрации на запрашивающий сервер УЦП-В; и вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации в соответствующем месте для будущего использования, причем сервер УЦП-В с сертификатом регистрации может использовать его для выдачи документов с УЦП в системе УЦП.

28. Способ по п.27, в котором сервер УЦП-Р не имеет действительных оснований для доверия серверу УЦП-В, при этом способ содержит этапы, на которых сервер УЦП-В обеспечивает представляющие его идентификационные данные, содержащие сертификат поручительства от стороны, желающей поручиться за такой сервер УЦП-В, причем сертификат поручительства включает в себя открытый ключ (PU-V) и соответствующий секретный ключ (PR-V); сервер УЦП-В использует (PU-E) и (PR-V) для формулирования признаков обладания, чтобы показать, что сервер УЦП-В обладает сертификатом поручительства;

сервер УЦП-В посылает запрос на регистрацию на сервер УЦП-Р, причем запрос включает в себя сертификат поручительства, (PU-E) и признаки обладания, сервер УЦП-Р проверяет подлинность сертификата поручительства, проверяет признаки обладания, и, если запрос должен быть удовлетворен, генерирует цифровой сертификат регистрации для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП, причем сгенерированный сертификат регистрации основан, по меньшей мере частично, на сертификате поручительства и (PU-E).

29. Способ по п.28, содержащий этап, на котором сервер УЦП-В обеспечивает сертификат поручительства от независимого выдающего сертификат агента, который является доверенным для сервера УЦП-Р и на который полагается сервер УЦП-Р в отношении выполнения такого поручительства.

30. Способ по п.28, содержащий этап, на котором сервер УЦП-В обеспечивает сертификат поручительства по стандарту X.509.

31. Способ по п.28, содержащий этапы, на которых сервер УЦП-В обеспечивает сертификат поручительства, подписанный поручающейся стороной и сопровождаемый цепочкой сертификатов, ведущей к известному корню, для целей проверки подлинности, сервер УЦП-Р проверяет подлинность сертификата поручительства на основе его подписи поручающейся стороной и цепочки сертификатов, чтобы убедиться в том, что за сервер УЦП-В внесено поручительство.

32. Способ по п.28, содержащий этапы, на которых сервер УЦП-В выполняет одну из следующих операций: использование (PR-V) для шифрования (PU-E), получая в результате (PR-V(PU-E)) в качестве признаков обладания, или подписание (PU-E) с помощью (PR-V), получая в результате (PU-E)S(PR-V) в качестве признаков обладания, сервер УЦП-Р проверяет признаки обладания посредством применения (PU-V) из запроса для дешифрования (PU-E) или проверки подписи, чтобы убедиться в том, что сервер УЦП-В обладает (PR-V) и, следовательно, сертификатом поручительства.

33. Способ по п.28, содержащий этап, на котором вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации, включающий в себя (PU-E) в качестве идентификатора сервера УЦП-В, идентифицирующие признаки для идентификации сертификата поручительства и подпись, основанную на секретном ключе сервера УЦП-Р, причем идентифицирующие признаки для сертификата поручительства в сертификате регистрации служат в качестве моста к сертификату поручительства и показывают, что сервер УЦП-Р доверяет и полагается на поручающуюся сторону в отношении поручительства за сервер УЦП-В.

34. Способ по п.33, содержащий этап, на котором вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации, дополнительно включающий в себя открытый ключ сервера УЦП-Р в качестве его идентификатора.

35. Способ по п.33, содержащий этап, на котором вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации, дополнительно включающий в себя информацию об интервале подлинности, задающую интервал, в течение которого сертификат регистрации является подлинным.

36. Способ по п.27, в котором сервер УЦП-Р имеет действительные основания для доверия серверу УЦП-В, при этом способ содержит этапы, на которых

сервер УЦП-В обеспечивает представляющие его идентификационные данные, содержащие мандат, который может быть опознан сервером УЦП-Р, принимает решение и подлинность которого, как ожидается, будет подтверждена сервером УЦП-Р;

сервер УЦП-В посылает запрос на регистрацию на сервер УЦП-Р, причем запрос включает в себя мандат и (PU-E), сервер УЦП-Р проверяет подлинность мандата и, если запрос должен быть удовлетворен, генерирует цифровой сертификат регистрации для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП, причем сгенерированный сертификат регистрации основан, по меньшей мере частично, на мандате и (PU-E).

37. Способ по п.36, содержащий этап, на котором сервер УЦП-В обеспечивает мандат, выбранный из группы, состоящей из идентификатора сети или идентификатора домена и мандата, выданного третьей стороной.

38. Способ по п.36, содержащий этап, на котором вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации, включающий в себя (PU-E) в качестве идентификатора сервера УЦП-В, идентифицирующие признаки для идентификации мандата и подпись, основанную на секретном ключе сервера УЦП-Р.

39. Способ по п.38, содержащий этап, на котором вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации, дополнительно включающий в себя открытый ключ сервера УЦП-Р в качестве его идентификатора.

40. Способ по п.38, содержащий этап, на котором вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации, дополнительно включающий в себя информацию об интервале подлинности, задающую интервал, в течение которого сертификат регистрации является подлинным.

41. Способ по п.27, содержащий этап, на котором вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации, включающий в себя (PU-E) в качестве идентификатора сервера УЦП-В и подпись, основанную на секретном ключе сервера УЦП-Р.

42. Способ по п.41, содержащий этап, на котором вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации, дополнительно включающий в

себя открытый ключ сервера УЦП-Р в качестве его идентификатора.

43. Способ по п.41, содержащий этап, на котором вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации, дополнительно включающий в себя информацию об интервале подлинности, задающую интервал, в течение которого сертификат регистрации является подлинным.

44. Способ по п.41, содержащий этап, на котором вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации, дополнительно включающий в себя идентифицирующие признаки для идентификации представляющих идентификационных данных.

45. Способ по п.27, содержащий этап, на котором вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации, включающий в себя цепочку сертификатов, которая ведет в обратном направлении к доверенному корневому органу, так что подлинность сгенерированного сертификата регистрации может быть проверена на основе такой цепочки сертификатов.

46. Способ по п.27, дополнительно содержащий этапы, на которых сервер УЦП-В идентифицирует в списке объектов с полномочиями аннулирования по меньшей мере один объект с полномочиями аннулирования регистрации такого сервера УЦП-В в системе УЦП, содержащий этап, на котором сервер УЦП-В посылает запрос на регистрацию на сервер УЦП-Р, причем запрос включает в себя представляющие идентификационные данные, (PU-E) и список объектов с полномочиями аннулирования, сервер УЦП-Р, если запрос должен быть удовлетворен, генерирует цифровой сертификат регистрации для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП, причем сгенерированный сертификат регистрации основан, по меньшей мере частично, на (PU-E) и списке объектов с полномочиями аннулирования.

47. Способ по п.46, содержащий этап, на котором сервер УЦП-В идентифицирует каждый объект в списке объектов с полномочиями аннулирования посредством его открытого ключа.

48. Способ по п.46, содержащий этап, на котором вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации, включающий в себя (PU-E) в качестве идентификатора сервера УЦП-В, список объектов с полномочиями аннулирования из запроса и подпись, основанную на секретном ключе сервера УЦП-Р.

49. Способ по п.27, содержащий этап, на котором вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации, хранящий сертификат регистрации, соответствующий XrML.

50. Способ регистрации входящего сервера управления цифровым правами (УЦП-В) в системе управления цифровыми правами (УЦП), имеющей множество серверов УЦП, выполняющих функциональные возможности УЦП, посредством регистрирующего сервера управления цифровыми правами (УЦП-Р), так что входящий сервер УЦП-В должен быть доверенным в системе и содержит этапы, на которых сервер УЦП-Р принимает запрос на регистрацию от сервера УЦП-В, включающий в себя представляющие идентификационные данные и открытый ключ сервера УЦП-В (PU-E) для идентификации такого сервера УЦП-В в системе УЦП;

сервер УЦП-Р проверяет подлинность представляющих идентификационных данных;

сервер УЦП-Р, если запрос должен быть удовлетворен, генерирует цифровой сертификат регистрации для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП, причем сгенерированный сертификат регистрации основан, по меньшей мере частично, на (PU-E); и

сервер УЦП-Р возвращает сгенерированный сертификат регистрации на запрашивающий сервер УЦП-В, вновь зарегистрированный сервер УЦП-В сохраняет возвращенный сертификат регистрации в соответствующем месте для будущего использования, причем сервер УЦП-В с сертификатом регистрации может использовать его для выдачи документов с УЦП в системе УЦП.

51. Способ по п.50, в котором сервер УЦП-Р не имеет действительных оснований для

доверия серверу УЦП-В, при этом способ содержит этапы, на которых сервер УЦП-Р принимает запрос на регистрацию от сервера УЦП-В, включающий в себя (PU-E) и представляющие идентификационные данные, содержащие сертификат поручительства от стороны, желающей поручиться за такой сервер УЦП-В, причем сертификат поручительства включает в себя открытый ключ (PU-V) и соответствующий секретный ключ (PR-V), причем сервер УЦП-В использует (PU-E) и (PR-V) для формулирования признаков обладания, чтобы показать, что сервер УЦП-В обладает сертификатом поручительства, а запрос на регистрацию дополнительно включает в себя признаки обладания; сервер УЦП-Р проверяет подлинность сертификата поручительства; сервер УЦП-Р проверяет признаки обладания; и

сервер УЦП-Р, если запрос должен быть удовлетворен, генерирует цифровой сертификат регистрации для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП, причем сгенерированный сертификат регистрации основан, по меньшей мере частично, на сертификате поручительства и (PU-E).

52. Способ по п.51, содержащий этап, на котором сервер УЦП-Р принимает запрос на регистрацию от сервера УЦП-В, включающий в себя сертификат поручительства от независимого выдающего сертификат агента, который является доверенным для сервера УЦП-Р и на который полагается сервер УЦП-Р в отношении выполнения такого поручительства.

53. Способ по п.51, содержащий этап, на котором сервер УЦП-Р принимает запрос на регистрацию от сервера УЦП-В, включающий в себя сертификат поручительства по стандарту X.509.

54. Способ по п.51, содержащий этапы, на которых сервер УЦП-Р принимает запрос на регистрацию от сервера УЦП-В, включающий в себя сертификат поручительства, подписанный поручающейся стороной и сопровождаемый цепочкой сертификатов, ведущей к известному корню, для целей проверки подлинности; и

сервер УЦП-Р проверяет подлинность сертификата поручительства на основе его подписи поручающейся стороной и цепочки сертификатов, чтобы убедиться в том, что за сервер УЦП-В внесено поручительство.

55. Способ по п.51, в котором сервер УЦП-В выполняет одну из следующих операций: использование (PR-V) для шифрования (PU-E), получая в результате (PR-V(PU-E)) в качестве признаков обладания, или подписание (PU-E) с помощью (PR-V), получая в результате (PU-E)S(PR-V) в качестве признаков обладания, при этом способ содержит этап, на котором сервер УЦП-Р проверяет признаки обладания посредством применения (PU-V) из запроса для дешифрования (PU-E) или проверки подписи, чтобы убедиться в том, что сервер УЦП-В обладает (PR-V) и, следовательно, сертификатом поручительства.

56. Способ по п.51, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации, включающий в себя (PU-E) в качестве идентификатора сервера УЦП-В, идентифицирующие признаки для идентификации сертификата поручительства и подпись, основанную на секретном ключе сервера УЦП-Р, при этом идентифицирующие признаки для сертификата поручительства в сертификате регистрации служат в качестве моста к сертификату поручительства и показывают, что сервер УЦП-Р доверяет и полагается на поручающуюся сторону в отношении поручительства за сервер УЦП-В.

57. Способ по п.56, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя открытый ключ сервера УЦП-Р в качестве его идентификатора.

58. Способ по п.56, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя информацию об интервале подлинности, задающую интервал, в течение которого сертификат регистрации является подлинным.

59. Способ по п.50, в котором сервер УЦП-Р имеет действительные основания для доверия серверу УЦП-В, при этом способ содержит этапы, на которых сервер УЦП-Р принимает запрос на регистрацию от сервера УЦП-В, включающий в себя (PU-E) и

представляющие идентификационные данные, содержащие мандат, который может быть опознан сервером УЦП-Р и подлинность которого, как ожидается, будет подтверждена сервером УЦП-Р; сервер УЦП-Р проверяет подлинность мандата; и сервер УЦП-Р, если запрос должен быть удовлетворен, генерирует цифровой сертификат регистрации для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП, причем сгенерированный сертификат регистрации основан, по меньшей мере частично, на мандате и (PU-E).

60. Способ по п.59, содержащий этап, на котором сервер УЦП-Р принимает запрос на регистрацию от сервера УЦП-В, включающий в себя мандат, выбранный из группы, состоящей из идентификатора сети или идентификатора домена и мандата, выданного третьей стороной.

61. Способ по п.59, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он включал в себя (PU-E) в качестве идентификатора сервера УЦП-В, идентифицирующие признаки для идентификации мандата и подпись, основанную на секретном ключе сервера УЦП-Р.

62. Способ по п.61, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя открытый ключ сервера УЦП-Р в качестве его идентификатора.

63. Способ по п.61, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя информацию об интервале подлинности, задающую интервал, в течение которого сертификат регистрации является подлинным.

64. Способ по п.50, дополнительно содержащий этап, на котором сервер УЦП-Р принимает решение в отношении того, удовлетворять ли запрос.

65. Способ по п.64, содержащий этап, на котором сервер УЦП-Р выполняет операции, выбранные из группы, состоящей из выполнения фоновой проверки сервера УЦП-В и/или его оператора, определения того, является ли текущим сервер УЦП-В и/или его часть, определения того, находится ли сервер УЦП-В в списке аннулирования или в списке, за которым ведется наблюдение, и комбинаций вышеперечисленного.

66. Способ по п.50, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он включал в себя (PU-E) в качестве идентификатора сервера УЦП-В и подпись, основанную на секретном ключе сервера УЦП-Р.

67. Способ по п.66, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя открытый ключ сервера УЦП-Р в качестве его идентификатора.

68. Способ по п.66, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя информацию об интервале подлинности, задающую интервал, в течение которого сертификат регистрации является подлинным.

69. Способ по п.66, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он дополнительно включал в себя идентифицирующие признаки для идентификации представляющих идентификационных данных.

70. Способ по п.50, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации посредством использования операций для генерирования по меньшей мере части информации в сертификате регистрации.

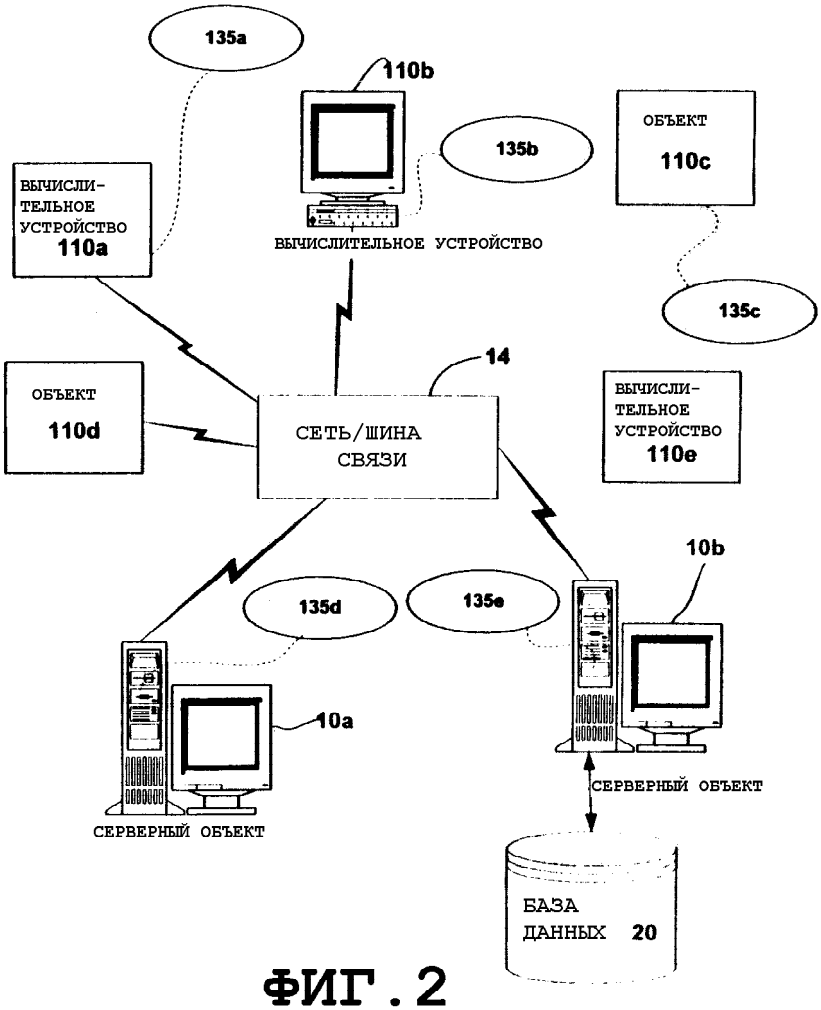
71. Способ по п.50, дополнительно содержащий этап, на котором сервер УЦП-Р присоединяет к сгенерированному сертификату регистрации цепочку сертификатов, которая ведет в обратном направлении к доверенному корневому органу, так что подлинность сгенерированного сертификата регистрации может быть проверена на основе такой цепочки сертификатов.

72. Способ по п.50, дополнительно содержащий этапы, на которых сервер УЦП-Р принимает запрос на регистрацию от сервера УЦП-В, дополнительно включающий в себя список объектов с полномочиями аннулирования, идентифицирующий по меньшей мере

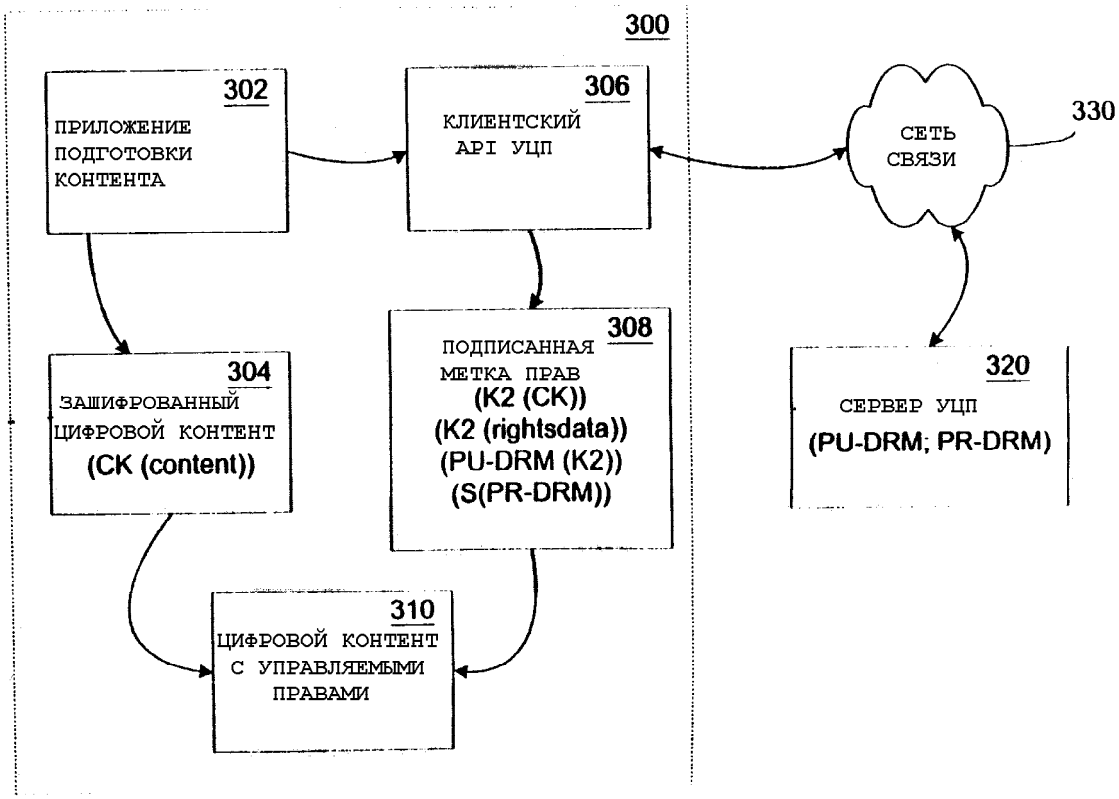
один объект с полномочиями аннулирования регистрации такого сервера УЦП-В в системе УЦП, и содержащий этап, на котором сервер УЦП-Р, если запрос должен быть удовлетворен, генерирует цифровой сертификат регистрации для сервера УЦП-В с целью регистрации такого сервера УЦП-В в системе УЦП, причем сгенерированный сертификат на регистрацию основан, по меньшей мере частично, на списке объектов с полномочиями аннулирования.

73. Способ по п.72, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации так, чтобы он включал в себя (PU-E) в качестве идентификатора сервера УЦП-В, список органов объектов с полномочиями аннулирования из запроса и подпись, основанную на секретном ключе сервера УЦП-Р.

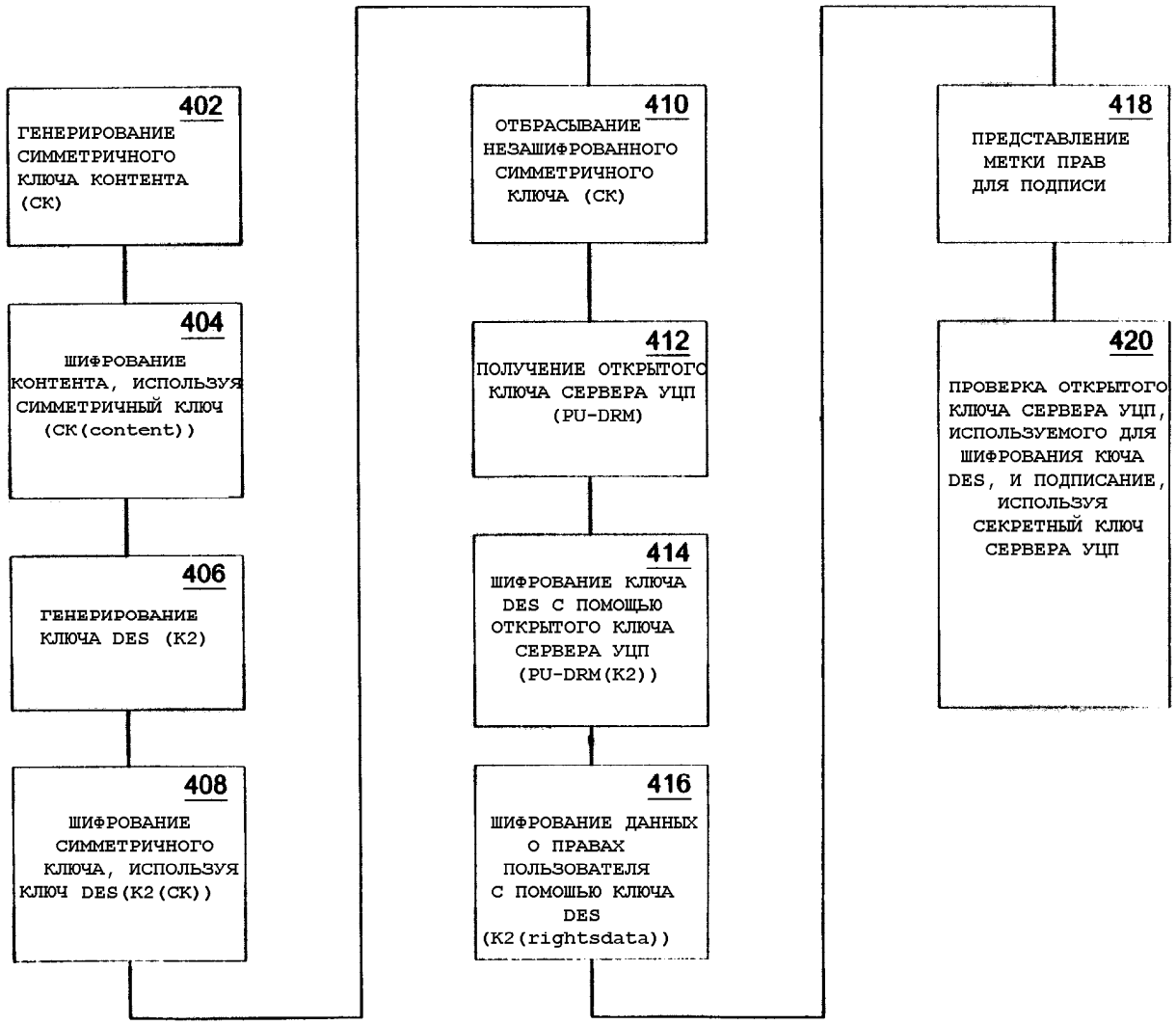
74. Способ по п.50, содержащий этап, на котором сервер УЦП-Р генерирует сертификат регистрации в соответствии с XrML.


135a
110b
135b
ОБЪЕКТ
110c
ВЫЧИСЛИ-
ТЕЛЬНОЕ
УСТРОЙСТВО
110a
ВЫЧИСЛИТЕЛЬНОЕ УСТРОЙСТВО
135c
14
ОБЪЕКТ
110d
СЕТЬ/ШИНА
СВЯЗИ
ВЫЧИСЛИ-
ТЕЛЬНОЕ
УСТРОЙСТВО
110e
10b
135d
135e
10a
СЕРВЕРНЫЙ ОБЪЕКТ
СЕРВЕРНЫЙ ОБЪЕКТ
БАЗА
ДАННЫХ 20

ФИГ. 2


300
302
ПРИЛОЖЕНИЕ
ПОДГОТОВКИ
КОНТЕНТА
306
КЛИЕНТСКИЙ
API УЦП
СЕТЬ
СВЯЗИ
330
308
ПОДПИСАННАЯ
МЕТКА ПРАВ
(K2 (CK))
(K2 (rightsdata))
(PU-DRM (K2))
(S(PR-DRM))
304
ЗАШИФРОВАННЫЙ
ЦИФРОВОЙ КОНТЕНТ
(CK (content))
320
СЕРВЕР УЦП
(PU-DRM; PR-DRM)
310
ЦИФРОВОЙ КОНТЕНТ
С УПРАВЛЯЕМЫМИ
ПРАВАМИ

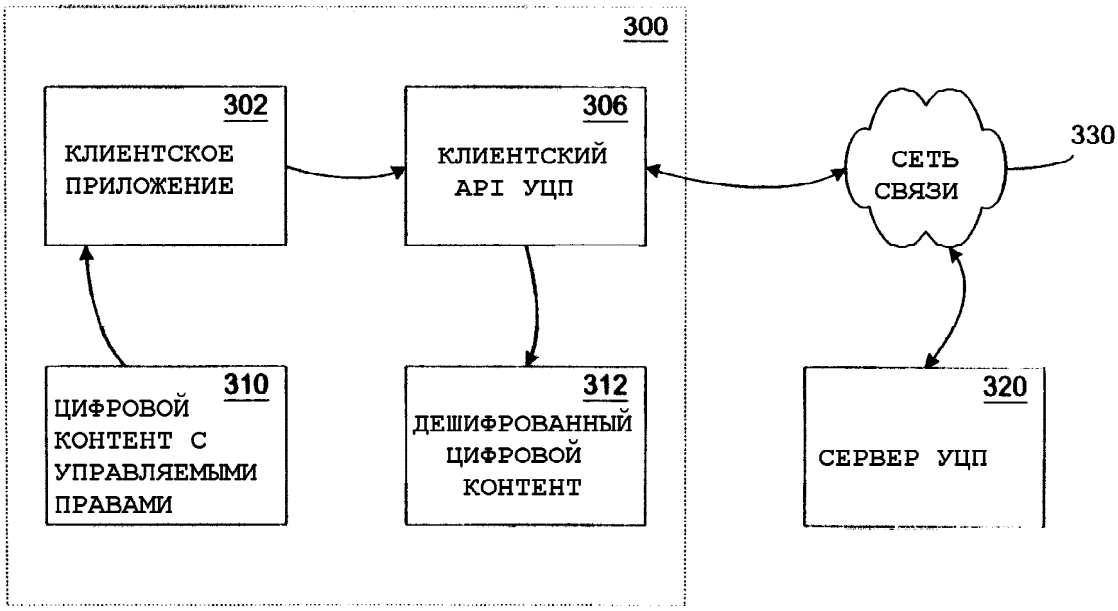
ФИГ. 3


402
ГЕНЕРИРОВАНИЕ СИММЕТРИЧНОГО КЛЮЧА КОНТЕНТА (СК)
404
ШИФРОВАНИЕ КОНТЕНТА, ИСПОЛЬЗУЯ СИММЕТРИЧНЫЙ КЛЮЧ (СК(content))
406
ГЕНЕРИРОВАНИЕ КЛЮЧА DES (К2)
408
ШИФРОВАНИЕ СИММЕТРИЧНОГО КЛЮЧА, ИСПОЛЬЗУЯ КЛЮЧ DES(К2(СК))
410
ОТБРАСЫВАНИЕ НЕЗАШИФРОВАННОГО СИММЕТРИЧНОГО КЛЮЧА (СК)
412
ПОЛУЧЕНИЕ ОТКРЫТОГО КЛЮЧА СЕРВЕРА УЦП (PU-DRM)
414
ШИФРОВАНИЕ КЛЮЧА DES С ПОМОЩЬЮ ОТКРЫТОГО КЛЮЧА СЕРВЕРА УЦП (PU-DRM(К2))
416
ШИФРОВАНИЕ ДАННЫХ О ПРАВАХ ПОЛЬЗОВАТЕЛЯ С ПОМОЩЬЮ КЛЮЧА DES (К2(rightsdata))
418
ПРЕДСТАВЛЕНИЕ МЕТКИ ПРАВ ДЛЯ ПОДПИСИ
420
ПРОВЕРКА ОТКРЫТОГО КЛЮЧА СЕРВЕРА УЦП, ИСПОЛЬЗУЕМОГО ДЛЯ ШИФРОВАНИЯ КЮЧА DES, И ПОДПИСАНИЕ, ИСПОЛЬЗУЯ СЕКРЕТНЫЙ КЛЮЧ СЕРВЕРА УЦП

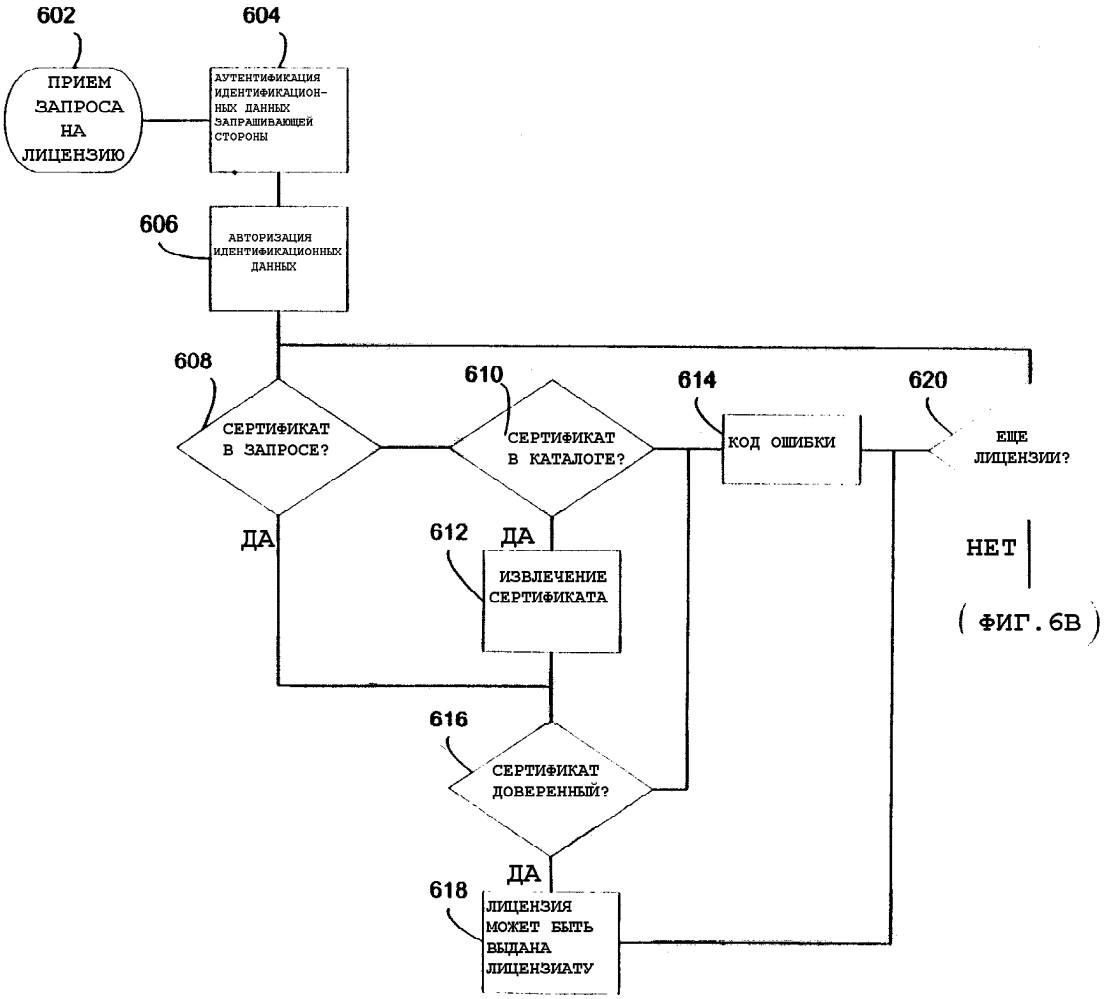
ФИГ. 4

ПМП 308
ИНФОРМАЦИЯ О КОНТЕНТЕ
ИНФОРМАЦИЯ О СЕРВЕРЕ УЦП
- (PU-DRM(K2))
-ССЫЛОЧНАЯ ИНФОРМАЦИЯ
- - URL
--ВОЗВРАТ В ИСХОДНОЕ СОСТОЯНИЕ
ИНФОРМАЦИЯ О МЕТКЕ ПРАВ
(K2(RIGHTSDATA))
(K2(CK))
S (PR-DRM)

ФИГ. 4А

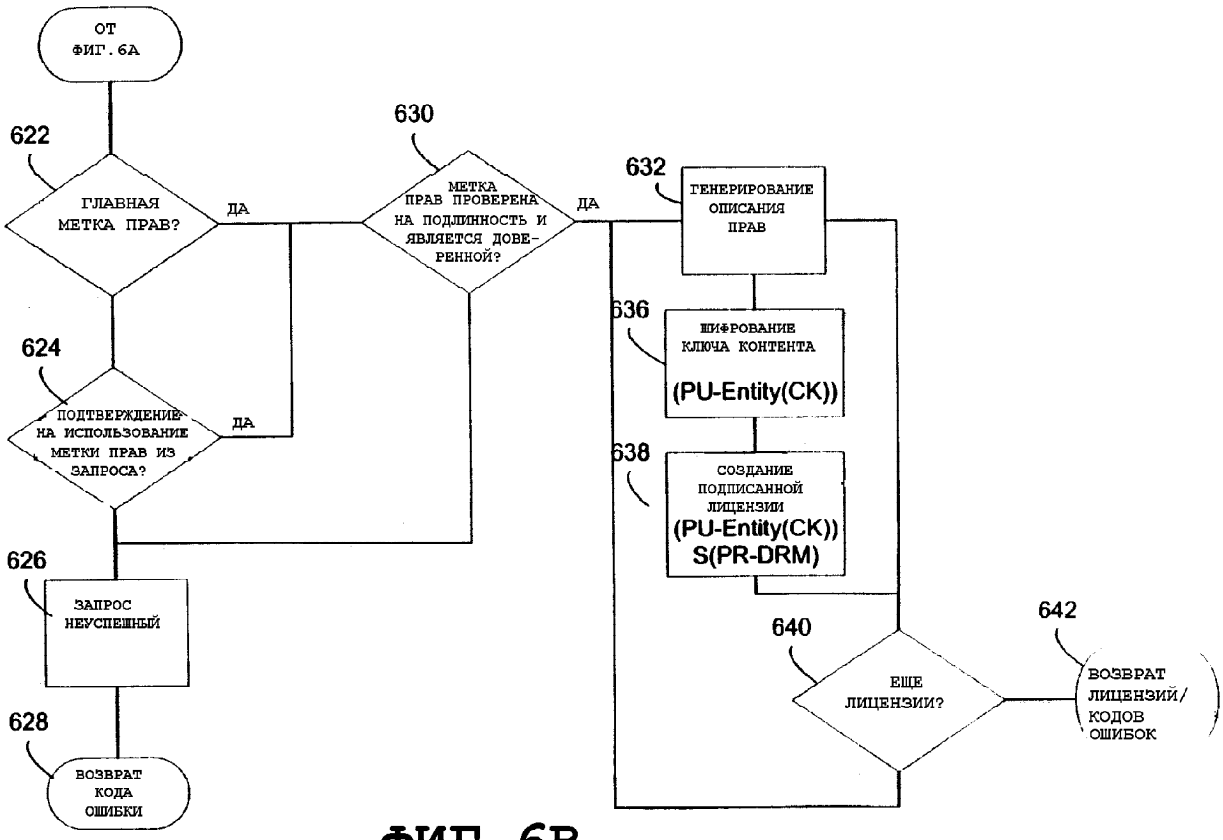


ФИГ. 5

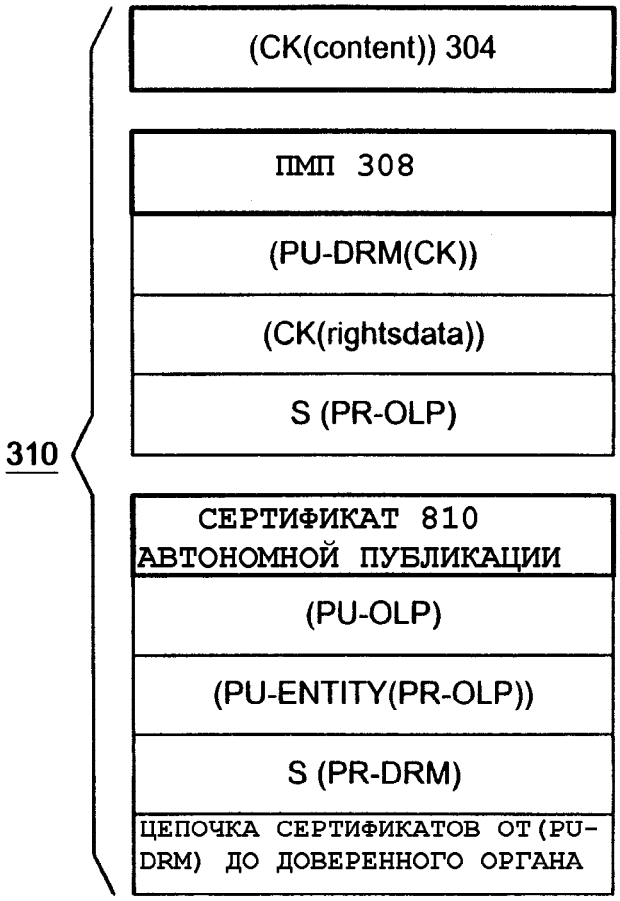


ФИГ. 6В

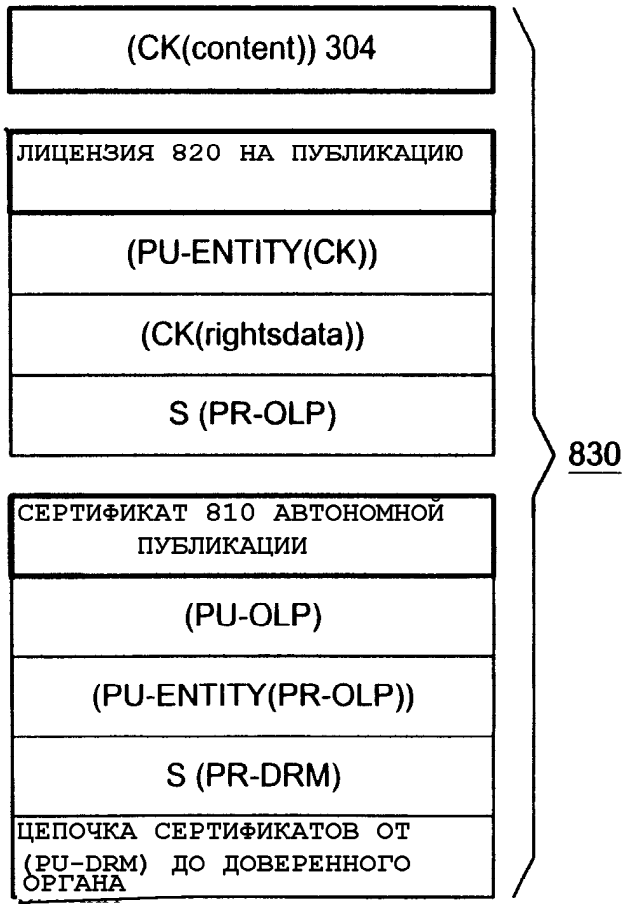
ФИГ. 6А



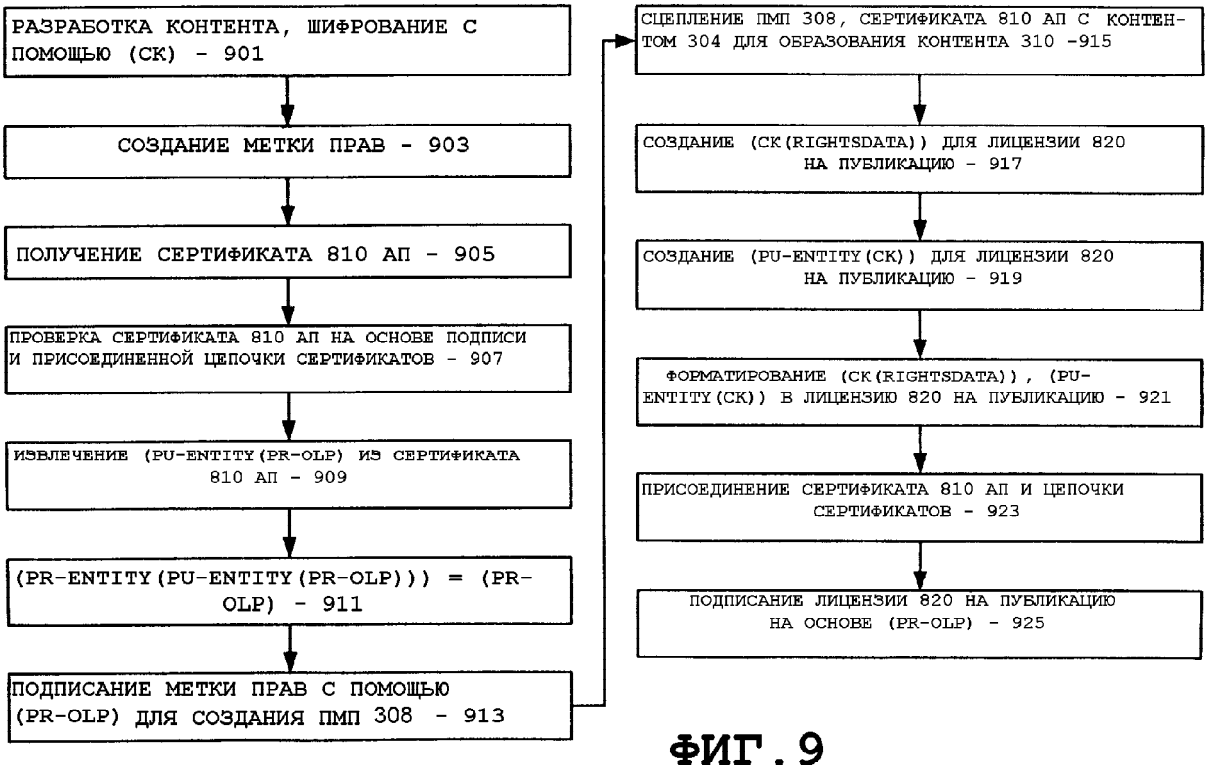
ФИГ. 6В


(CK(content)) 304
ПМП 308
(PU-DRM(CK))
(CK(rightsdata))
S (PR-OLP)
310
СЕРТИФИКАТ 810 АВТОНОМНОЙ ПУБЛИКАЦИИ
(PU-OLP)
(PU-ENTITY(PR-OLP))
S (PR-DRM)
ЦЕПОЧКА СЕРТИФИКАТОВ ОТ (PU-DRM) ДО ДОВЕРЕННОГО ОРГАНА

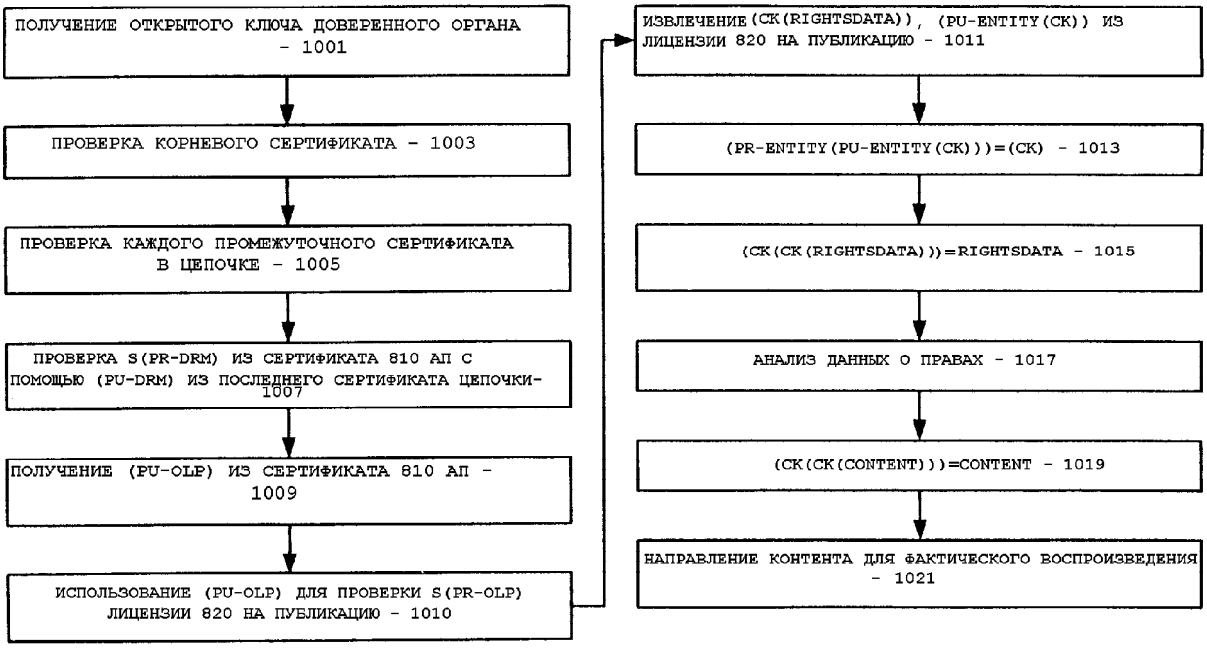
ФИГ. 7


(CK(content)) 304
ЛИЦЕНЗИЯ 820 НА ПУБЛИКАЦИЮ
(PU-ENTITY(CK))
(CK(rightsdata))
S (PR-OLP)
830
СЕРТИФИКАТ 810 АВТОНОМНОЙ ПУБЛИКАЦИИ
(PU-OLP)
(PU-ENTITY(PR-OLP))
S (PR-DRM)
ЦЕПОЧКА СЕРТИФИКАТОВ ОТ (PU-DRM) ДО ДОВЕРЕННОГО ОРГАНА

ФИГ. 8

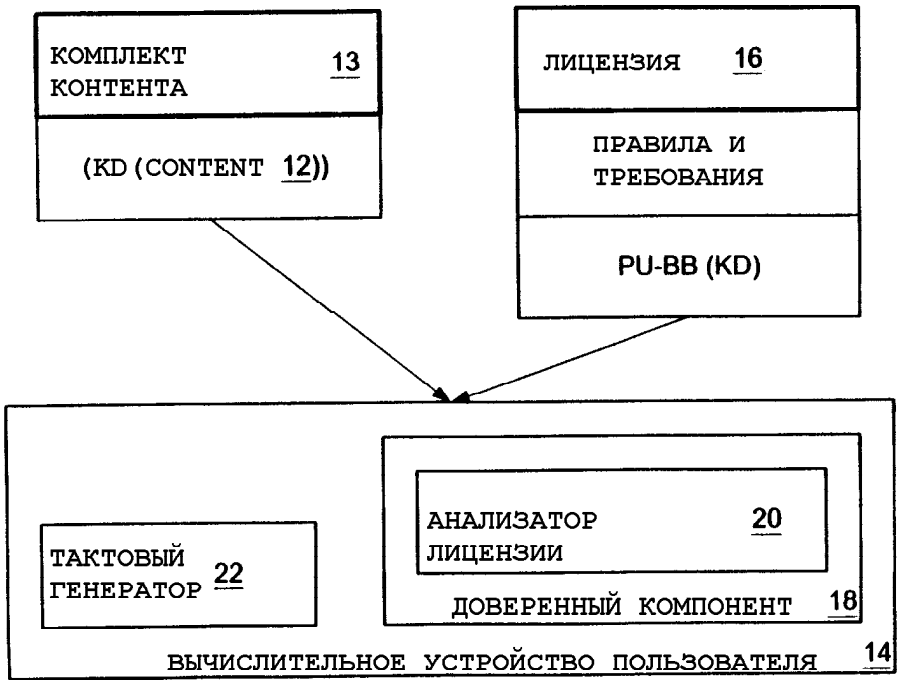

РАЗРАБОТКА КОНТЕНТА, ШИФРОВАНИЕ С ПОМОЩЬЮ (CK) - 901
СОЗДАНИЕ МЕТКИ ПРАВ - 903
ПОЛУЧЕНИЕ СЕРТИФИКАТА 810 АП - 905
ПРОВЕРКА СЕРТИФИКАТА 810 АП НА ОСНОВЕ ПОДПИСИ И ПРИСОЕДИНЕННОЙ ЦЕПОЧКИ СЕРТИФИКАТОВ - 907
ИЗВЛЕЧЕНИЕ (PU-ENTITY(PR-OLP) ИЗ СЕРТИФИКАТА 810 АП - 909
(PR-ENTITY(PU-ENTITY(PR-OLP))) = (PR-OLP) - 911
ПОДПИСАНИЕ МЕТКИ ПРАВ С ПОМОЩЬЮ (PR-OLP) ДЛЯ СОЗДАНИЯ ПМП 308 - 913
СЦЕПЛЕНИЕ ПМП 308, СЕРТИФИКАТА 810 АП С КОНТЕНТОМ 304 ДЛЯ ОБРАЗОВАНИЯ КОНТЕНТА 310 -915
СОЗДАНИЕ (CK(RIGHTSDATA)) ДЛЯ ЛИЦЕНЗИИ 820 НА ПУБЛИКАЦИЮ - 917
СОЗДАНИЕ (PU-ENTITY(CK)) ДЛЯ ЛИЦЕНЗИИ 820 НА ПУБЛИКАЦИЮ - 919
ФОРМАТИРОВАНИЕ (CK(RIGHTSDATA)), (PU-ENTITY(CK)) В ЛИЦЕНЗИЮ 820 НА ПУБЛИКАЦИЮ - 921
ПРИСОЕДИНЕНИЕ СЕРТИФИКАТА 810 АП И ЦЕПОЧКИ СЕРТИФИКАТОВ - 923
ПОДПИСАНИЕ ЛИЦЕНЗИИ 820 НА ПУБЛИКАЦИЮ НА ОСНОВЕ (PR-OLP) - 925

ФИГ. 9

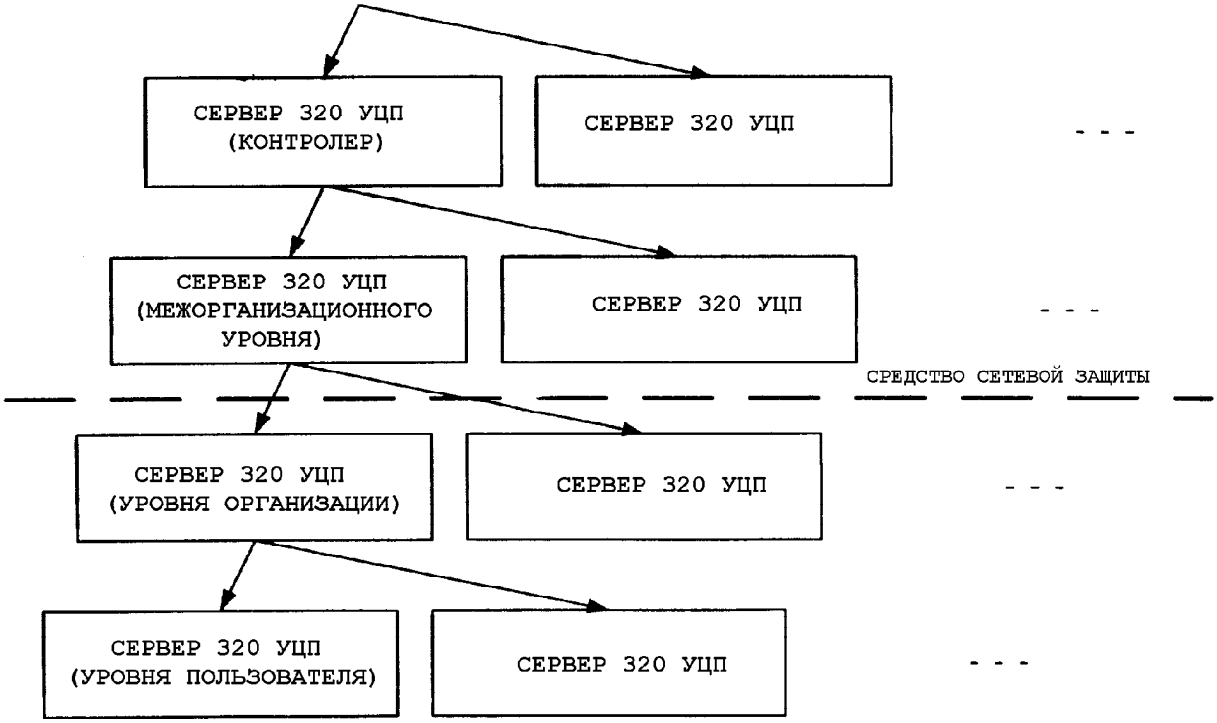


ФИГ.10

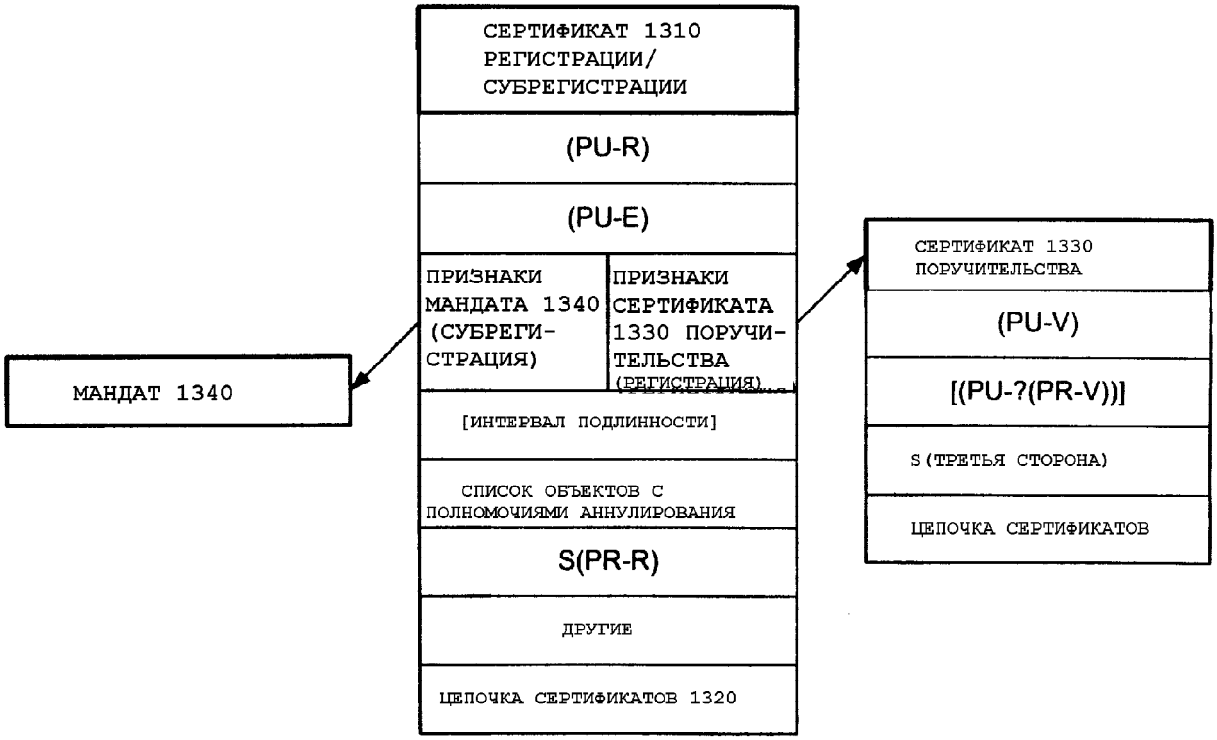
СИСТЕМА УЦП 10



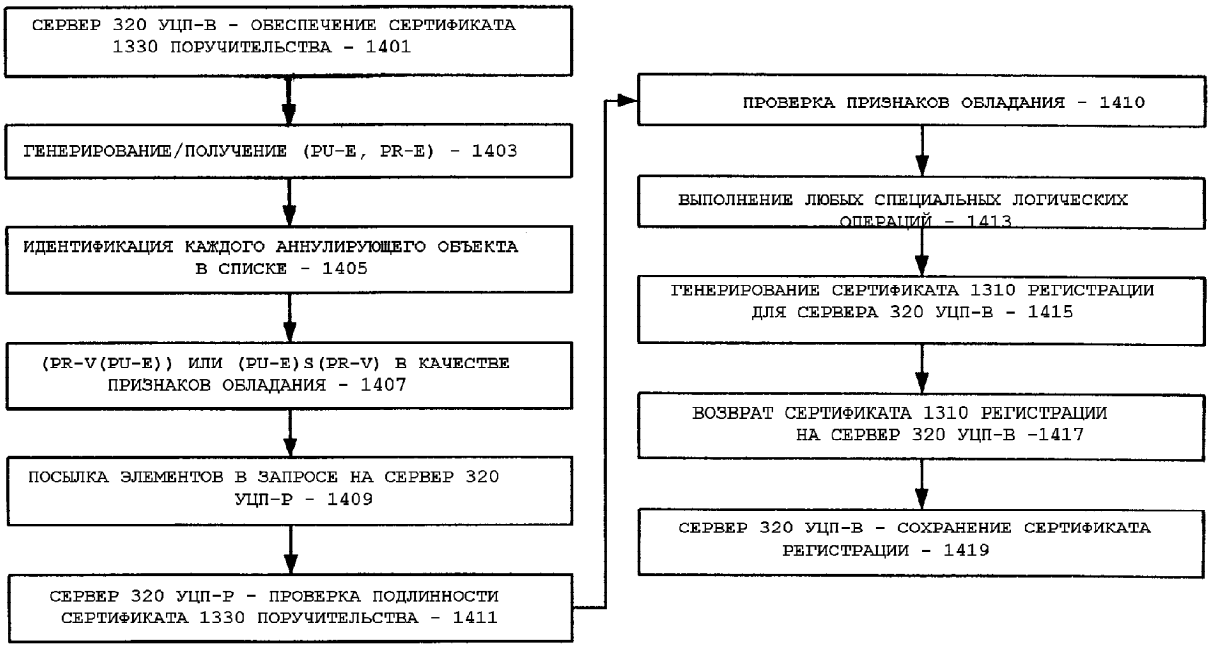
ФИГ.11


СЕРВЕР 320 УЦП (КОНТРОЛЕР)
СЕРВЕР 320 УЦП
СЕРВЕР 320 УЦП (МЕЖОРГАНИЗАЦИОННОГО УРОВНЯ)
СЕРВЕР 320 УЦП
СРЕДСТВО СЕТЕВОЙ ЗАЩИТЫ
СЕРВЕР 320 УЦП (УРОВНЯ ОРГАНИЗАЦИИ)
СЕРВЕР 320 УЦП
СЕРВЕР 320 УЦП (УРОВНЯ ПОЛЬЗОВАТЕЛЯ)
СЕРВЕР 320 УЦП

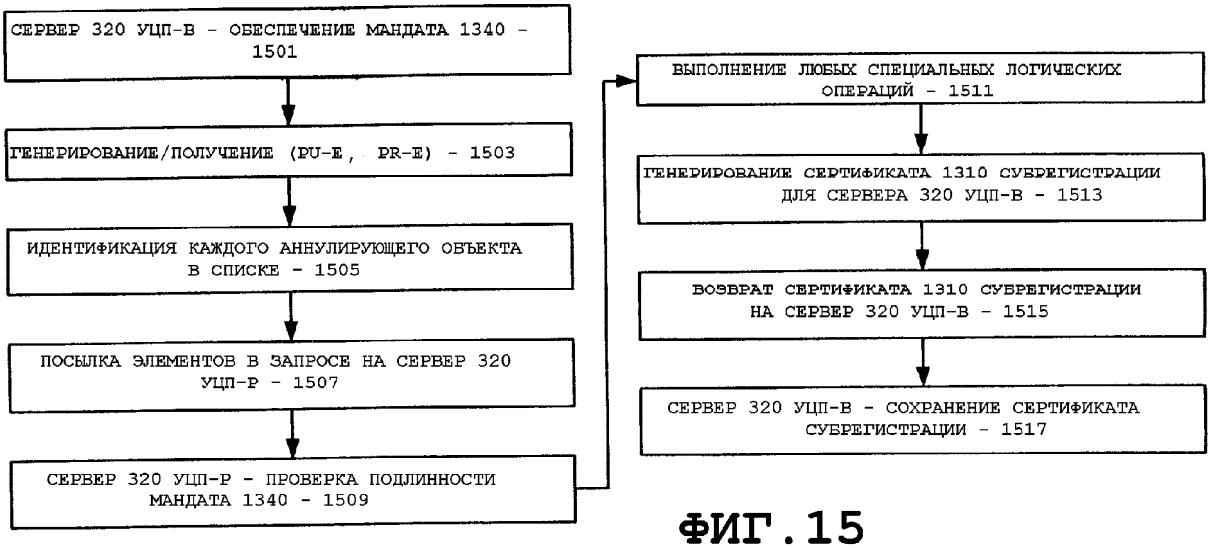
ФИГ.12


СЕРТИФИКАТ 1310 РЕГИСТРАЦИИ/ СУБРЕГИСТРАЦИИ
(PU-R)
(PU-E)
ПРИЗНАКИ МАНДАТА 1340 (СУБРЕГИ-СТРАЦИЯ)
ПРИЗНАКИ СЕРТИФИКАТА 1330 ПОРУЧИ-ТЕЛЬСТВА (РЕГИСТРАЦИЯ)
[ИНТЕРВАЛ ПОДЛИННОСТИ]
СПИСОК ОБЪЕКТОВ С ПОЛНОМОЧИЯМИ АННУЛИРОВАНИЯ
S(PR-R)
ДРУГИЕ
ЦЕПОЧКА СЕРТИФИКАТОВ 1320
МАНДАТ 1340
СЕРТИФИКАТ 1330 ПОРУЧИТЕЛЬСТВА
(PU-V)
[(PU-?(PR-V))]
S(ТРЕТЬЯ СТОРОНА)
ЦЕПОЧКА СЕРТИФИКАТОВ

ФИГ.13


СЕРВЕР 320 УЦП-В - ОБЕСПЕЧЕНИЕ СЕРТИФИКАТА 1330 ПОРУЧИТЕЛЬСТВА - 1401
ГЕНЕРИРОВАНИЕ/ПОЛУЧЕНИЕ (PU-E, PR-E) - 1403
ИДЕНТИФИКАЦИЯ КАЖДОГО АННУЛИРУЮЩЕГО ОБЪЕКТА В СПИСКЕ - 1405
(PR-V(PU-E)) ИЛИ (PU-E)S(PR-V) В КАЧЕСТВЕ ПРИЗНАКОВ ОБЛАДАНИЯ - 1407
ПОСЫЛКА ЭЛЕМЕНТОВ В ЗАПРОСЕ НА СЕРВЕР 320 УЦП-Р - 1409
СЕРВЕР 320 УЦП-Р - ПРОВЕРКА ПОДЛИННОСТИ СЕРТИФИКАТА 1330 ПОРУЧИТЕЛЬСТВА - 1411
ПРОВЕРКА ПРИЗНАКОВ ОБЛАДАНИЯ - 1410
ВЫПОЛНЕНИЕ ЛЮБЫХ СПЕЦИАЛЬНЫХ ЛОГИЧЕСКИХ ОПЕРАЦИЙ - 1413
ГЕНЕРИРОВАНИЕ СЕРТИФИКАТА 1310 РЕГИСТРАЦИИ ДЛЯ СЕРВЕРА 320 УЦП-В - 1415
ВОЗВРАТ СЕРТИФИКАТА 1310 РЕГИСТРАЦИИ НА СЕРВЕР 320 УЦП-В -1417
СЕРВЕР 320 УЦП-В - СОХРАНЕНИЕ СЕРТИФИКАТА РЕГИСТРАЦИИ - 1419

ФИГ.14


СЕРВЕР 320 УЦП-В - ОБЕСПЕЧЕНИЕ МАНДАТА 1340 - 1501
ГЕНЕРИРОВАНИЕ/ПОЛУЧЕНИЕ (PU-E, PR-E) - 1503
ИДЕНТИФИКАЦИЯ КАЖДОГО АННУЛИРУЮЩЕГО ОБЪЕКТА В СПИСКЕ - 1505
ПОСЫЛКА ЭЛЕМЕНТОВ В ЗАПРОСЕ НА СЕРВЕР 320 УЦП-Р - 1507
СЕРВЕР 320 УЦП-Р - ПРОВЕРКА ПОДЛИННОСТИ МАНДАТА 1340 - 1509
ВЫПОЛНЕНИЕ ЛЮБЫХ СПЕЦИАЛЬНЫХ ЛОГИЧЕСКИХ ОПЕРАЦИЙ - 1511
ГЕНЕРИРОВАНИЕ СЕРТИФИКАТА 1310 СУБРЕГИСТРАЦИИ ДЛЯ СЕРВЕРА 320 УЦП-В - 1513
ВОЗВРАТ СЕРТИФИКАТА 1310 СУБРЕГИСТРАЦИИ НА СЕРВЕР 320 УЦП-В - 1515
СЕРВЕР 320 УЦП-В - СОХРАНЕНИЕ СЕРТИФИКАТА СУБРЕГИСТРАЦИИ - 1517

ФИГ.15