РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 512 118**(13) **C2**

(51) МПК
G06F 21/30 (2013.01)
G06F 21/44 (2013.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2011105187/08, 24.07.2009**

(24) Дата начала отсчета срока действия патента:
24.07.2009

Приоритет(ы):
(30) Конвенционный приоритет:
14.08.2008 US 12/191,752

(43) Дата публикации заявки: **20.08.2012** Бюл. № **23**

(45) Опубликовано: **10.04.2014** Бюл. № **10**

(56) Список документов, цитированных в отчете о поиске: **US 2006/0085639 A1, 20.04.2006. US 2006/0064493 A1, 23.03.2006. US 6487660 B1, 26.11.2002. EP 1832998 A1, 12.09.2007. RU 61491 U1, 27.02.2007**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **11.02.2011**

(86) Заявка PCT:
US 2009/051628 (24.07.2009)

(87) Публикация заявки PCT:
WO 2010/019370 (18.02.2010)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, строение 3, ООО "Юридическая фирма Городисский и Партнеры"

(72) Автор(ы):
ГАНАПАТХИ Нараянан (US)

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

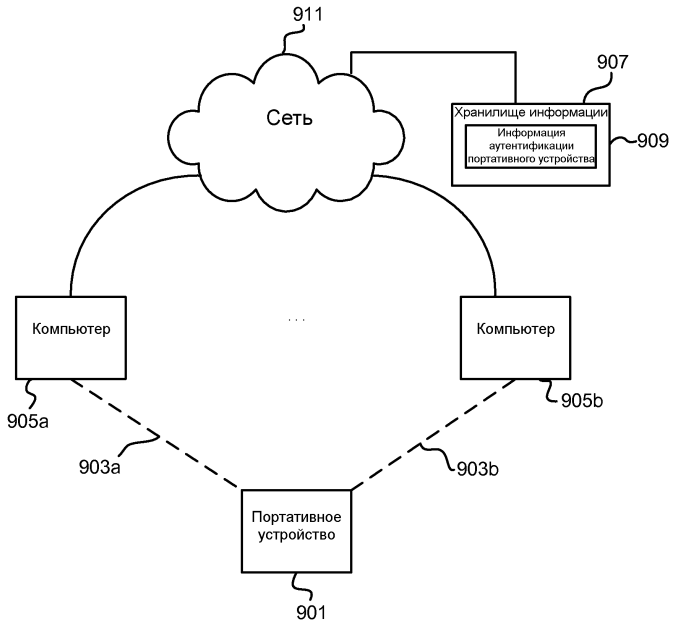
RU 2512118 C2

(54) ПРОТОКОЛ ПРИВЯЗКИ УСТРОЙСТВА К СТАНЦИИ

(57) Реферат:

Изобретение относится к системам и способам для безопасной привязки (или сопряжения) портативных электронных устройств к одному или более вычислительным устройствам. Технический результат заключается в автоматической привязке портативного устройства к двум или более разным компьютерам. Предложена методика, которая позволяет автоматически привязать портативное устройство к множеству компьютеров. Информация, которую компьютер может использовать, чтобы аутентифицировать портативное устройство и создать доверительное отношение до момента создания привязки к портативному устройству, создается и сохраняется в хранилище данных, которое доступно для множества компьютеров и ассоциировано с пользователем портативного устройства. В том случае, когда компьютер обнаруживает такое портативное устройство, с которым у него до сих пор нет привязки, компьютер может идентифицировать пользователя, вошедшего в систему компьютера, и использовать информацию, идентифицирующую пользователя, чтобы получить информацию аутентификации, которая является независящей

от устройства, и, как ожидается, будет представлена портативным устройством, чтобы аутентифицировать его и разрешить автоматическую привязку. 3 н. и 17 з.п. ф-лы, 12 ил.



ФИГ. 2

RU 2512118 C2

RU 2512118 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 512 118** (13) **C2**

(51) Int. Cl.
G06F 21/30 (2013.01)
G06F 21/44 (2013.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2011105187/08, 24.07.2009**

(24) Effective date for property rights:
24.07.2009

Priority:
(30) Convention priority:
14.08.2008 US 12/191,752

(43) Application published: **20.08.2012** Bull. № **23**

(45) Date of publication: **10.04.2014** Bull. № **10**

(85) Commencement of national phase: **11.02.2011**

(86) PCT application:
US 2009/051628 (24.07.2009)

(87) PCT publication:
WO 2010/019370 (18.02.2010)

Mail address:
129090, Moskva, ul. B. Spasskaja, 25, stroenie 3, OOO "Juridicheskaja firma Gorodisskij i Partnery"

(72) Inventor(s):
GANAPATKhI Narajanan (US)

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

RU 2512118 C2

(54) PROTOCOL FOR DEVICE TO STATION ASSOCIATION

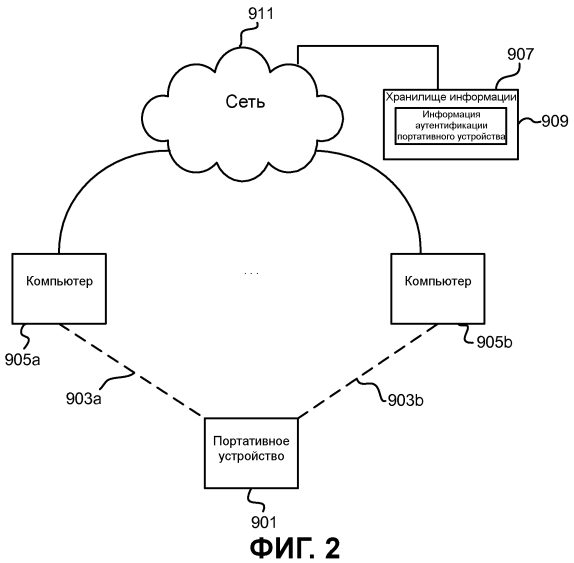
(57) Abstract:

FIELD: physics, computer technology.

SUBSTANCE: invention relates to systems and methods for secure association (or interfacing) of portable electronic devices to one or more computing devices. Disclosed is a technique which enables to automatically associate a portable device to a plurality of computers. Information that a computer can use to authenticate a portable device and establish a trusted relationship prior to creating an association with the portable device is created and stored in a data storage which is accessible for a plurality of computers and is associated with a user of the portable device. When a computer discovers such a portable device with which it is not yet associated, the computer can identify a user logged into the computer system and use information identifying the user to retrieve authentication information that is device independent and is expected to be presented by the portable device to authenticate it and allow automatic association.

EFFECT: facilitating automatic association of a portable device to two more different computers.

20 cl, 12 dwg



ФИГ. 2

RU 2512118 C2

Предпосылки создания изобретения

[0001] Изобретение относится к системам и способам для безопасной привязки (или сопряжения) портативных электронных устройств к одному или более вычислительным устройствам.

[0002] Пользователи все больше и больше эксплуатируют портативные электронные устройства разнообразных типов совместно с их компьютерами (например, беспроводные наушники, цифровые фотоаппараты, персональные цифровые помощники (PDA), мобильные телефоны, манипуляторы типа мышь и т.д.). Многие портативные электронные устройства выполнены с возможностью использования беспроводных технологий малого радиуса действия, таких как Bluetooth, ультраширокополосной радиосвязи (UWB), беспроводной универсальной последовательной шины (USB) и Связи в Ближнем Поле (NFC), в то время как прочие могут осуществлять связь с вычислительным устройством через физическое проводное соединение.

[0003] Беспроводные технологии малого радиуса действия и проводные соединения позволяют осуществлять связь только между устройствами, размещенными близко друг к другу. По причине этого ограничения в отношении физической близости, угрозы безопасности являются отчасти сниженными. То есть требуется, чтобы атакующее устройство было физически соединено с целевым вычислительным устройством или находилось в пределах его дальности передачи, чтобы иметь возможность перехватывать и/или внедрить сообщения. Несмотря на это, чтобы гарантировать, что вычислительное устройство привязывается и осуществляет связь только с доверенным и авторизованным устройством, как правило, используются функции обеспечения безопасности.

[0004] Обычно выполняется процесс, чтобы гарантировать, что портативное устройство является доверенным до момента, когда оно будет привязано к вычислительному устройству. Например, вычислительное устройство с реализованной беспроводной технологией может выполнять протокол обнаружения, чтобы получить список прочих устройств, на которых реализована та же технология и которые находятся в пределах дальности связи. Затем вычислительное устройство может инициировать как автоматически, так и по запросу пользователя сеанс связи с одним из обнаруженных устройств. Чтобы создать доверие между двумя устройствами, как правило, пользователю предлагается взаимодействовать с одним или обоими устройствами. Например, каждое устройство может отобразить цифровое значение, и пользователю предлагается ввести «да» на одном или обоих устройствах, если два отображаемых цифровых значения совпадают, чтобы тем самым удостовериться в том, что пользователь управляет обоими устройствами, то есть, что портативное устройство является доверенным. Такой процесс аутентификации при помощи пользователя, как правило, именуется «сопряжением вручную», так как он требует подтверждающего действия со стороны пользователя, выполненного вручную.

[0005] В качестве части обычного процесса сопряжения вручную, как только пользователь подтверждает, что соединение осуществляется между доверенными устройствами, устройства сохраняют информацию безопасности (например, ключевые материалы шифрования) для использования при последующей связи таким образом, что дальнейшая привязка между устройствами может выполняться устройствами автоматически, не требуя действий со стороны пользователя. Следовательно, если в дальнейшем два устройства обнаруживают друг друга, может быть найдена и произведен обмен сохраненной информацией безопасности, чтобы предоставить устройствам возможность распознать друг друга в качестве доверенных, не требуя выполнения другой процедуры сопряжения вручную.

Краткое описание сущности изобретения

[0006] Аспекты настоящего изобретения направлены на улучшение методик автоматической привязки портативного устройства (например, беспроводного устройства, такого как мобильный телефон, проигрыватель MP3, беспроводные наушники) к двум или более разным компьютерам. При использовании обычных методик требуется, чтобы было вручную создано сопряжение портативного устройства и компьютера, чтобы создать доверительное отношение между ними, чтобы в свою очередь способствовать последующей автоматической привязке, и требуется, чтобы процесс сопряжения вручную выполнялся отдельно для каждого компьютера, с которым пользователь желает использовать портативное устройство. Например, пользователю, который купил новые беспроводные наушники и планирует использовать их как на рабочем, так и домашнем компьютере, обычно требуется выполнить процесс сопряжения вручную с каждым из этих компьютеров, чтобы создать доверительное отношение с беспроводными наушниками. В качестве части процесса сопряжения вручную, производится обмен информацией аутентификации между компьютером и портативным устройством (например, беспроводными наушниками), которая может в дальнейшем использоваться, чтобы позволить устройствам аутентифицировать друг друга и создать автоматическую привязку. Вследствие этого, после того как вручную было осуществлено сопряжение устройства и компьютера, то как только в дальнейшем устройства попадают в пределы дальности связи, они могут аутентифицировать друг друга, чтобы создать доверительное отношение и автоматически установить связь.

[0007] Недостаток обычных методик состоит в том, что они требуют выполнения отдельных операций сопряжения вручную портативного устройства с каждым компьютером, с которым оно должно использоваться, что может быть обременительным для пользователя, в частности для пользователей, которые используют большое число портативных устройств с многочисленными компьютерами. В соответствии с одним вариантом осуществления изобретения устраняется необходимость в выполнении многочисленных операций сопряжения вручную. Это может быть достигнуто любым из нескольких способов. В одном аспекте, во время операции сопряжения вручную с первым компьютером, создается информация аутентификации между портативным устройством и пользователем компьютера, с которым производится сопряжение вручную устройства. Затем информация аутентификации сохраняется в глобально доступном для любого числа компьютеров хранилище информации. Следовательно, после того как была создана информация аутентификации, когда пользователь планирует использовать портативное устройство с любым новым компьютером (включая компьютер, с которым ранее не производилось сопряжение вручную), этот компьютер может получить информацию аутентификации из глобально доступного хранилища на основании идентификационных данных пользователя, вошедшего в систему компьютера, и может использовать эту информацию аутентификации, чтобы позволить новому компьютеру и портативному устройству автоматически аутентифицировать друг друга и создать привязку, не требуя, чтобы между ними было осуществлено сопряжение вручную. Это является преимуществом, так как пользователю необходимо лишь осуществить сопряжение вручную портативного устройства с одним компьютером, и позволяет устройству впоследствии быть автоматически привязанным к любому компьютеру, в систему которого входит пользователь, нежели требуя, чтобы пользователь впоследствии производил операции сопряжения вручную для каждого компьютера, с которым пользователь планирует использовать портативное устройство.

[0008] В альтернативном аспекте, информация аутентификации может быть создана

и предоставлена в глобально доступном хранилище, не требуя сопряжения вручную портативного устройства с каким-либо конкретным компьютером.

[0009] Другой вариант осуществления изобретения направлен на протокол для аутентификации портативного устройства с компьютером, используя информацию аутентификации, которая привязана к пользователю компьютера, нежели к самому конкретному компьютеру, так что информация аутентификации может использоваться любым компьютером, в систему которого вошел пользователь.

Перечень фигур чертежей

[0010] Прилагаемые чертежи не предназначены быть начерченными в масштабе. В чертежах, каждый одинаковый или близкий к одинаковому компонент, который иллюстрируется на разных фигурах, представлен одинаковым цифровым обозначением. В целях ясности, не каждый компонент может быть обозначен на каждом чертеже. На чертежах:

[0011] Фиг.1 иллюстрирует операцию сопряжения вручную мобильного устройства с одним компьютером и последующую автоматическую привязку к дополнительным компьютерам в соответствии с одним вариантом осуществления настоящего изобретения;

[0012] Фиг.2 иллюстрирует компьютерную систему, которая включает в себя глобально доступное хранилище информации, которое в свою очередь включает в себя информацию в отношении одного или более компьютеров, чтобы автоматически аутентифицировать и привязывать портативное устройство в соответствии с одним вариантом осуществления настоящего изобретения;

[0013] Фиг.3 является логической блок-схемой характерного процесса для создания и использования информации аутентификации для автоматической привязки портативного устройства к компьютеру в соответствии с одним вариантом осуществления настоящего изобретения;

[0014] Фиг.4 является процессом для создания информации аутентификации применительно к портативному устройству и для ее сохранения таким образом, который делает ее доступной для множества компьютеров в соответствии с одним вариантом осуществления настоящего изобретения;

[0015] Фиг.5 является процессом для автоматической привязки портативного устройства к компьютеру посредством идентификации пользователя, вошедшего в систему компьютера, и получения информации аутентификации, привязанной к пользователю, чтобы аутентифицировать портативное устройство в соответствии с одним вариантом осуществления изобретения;

[0016] Фиг.6 является обычным процессом для выполнения привязки устройства, прошедшего аутентификацию;

[0017] Фиг.7 иллюстрирует процесс сопряжения вручную компьютера с портативным устройством, чтобы создать информацию аутентификации в соответствии с одним вариантом осуществления настоящего изобретения;

[0018] Фиг.8 иллюстрирует характерную реализацию хранилища информации, которое включает в себя информацию аутентификации в отношении множества пользователей и портативных устройств в соответствии с одним вариантом осуществления настоящего изобретения;

[0019] Фиг.9 иллюстрирует характерную реализацию хранилища информации на портативном устройстве, которое включает в себя информацию, чтобы аутентифицировать портативное устройство по отношению к компьютеру на основании идентификационных данных пользователя компьютера;

[0020] Фиг.10 иллюстрирует процесс для получения профилей для аутентификации портативного устройства и компьютера в соответствии с одним вариантом осуществления настоящего изобретения;

[0021] Фиг.11 является схемой, которая иллюстрирует пример протокола для осуществления связи между компьютером и портативным устройством, чтобы произвести взаимную аутентификацию компьютера и портативного устройства и предоставить возможность автоматической их привязки в соответствии с одним вариантом осуществления настоящего изобретения; и

[0022] Фиг.12 является схематической иллюстрацией характерного компьютера, на котором могут быть реализованы аспекты настоящего изобретения.

Подробное описание

[0023] В соответствии с тем, что рассматривалось выше, обычные протоколы привязки устройства основываются на вмешательстве пользователя в ручном режиме, чтобы исходно создать доверие между двумя устройствами. Информация аутентификации (например, ключевые материалы шифрования), созданная или полученная путем обмена во время начальной процедуры сопряжения вручную, затем может быть использована, чтобы в дальнейшем предоставить двум устройствам, которые были привязаны в прошлом, возможность быть привязанными автоматически без вмешательства пользователя. Тем не менее, процедура сопряжения вручную должна быть выполнена, по меньшей мере, один раз, чтобы обеспечить обмен требуемой информацией безопасности для любых двух устройств, которые никогда не были привязаны.

[0024] Заявители исходят из того, что некоторые пользователи используют два или более разные вычислительные устройства (например, одно дома, а другое на работе), к которым пользователь хотел бы привязать то же самое одно или более портативное устройство(а) (например, наушники, проигрыватель MP3, мобильный телефон и т.д.). Заявители дополнительно исходят из того, что процесс сопряжения вручную может быть трудоемким и обременительным для пользователей устройств, в частности, когда требуется, чтобы он повторялся множество раз применительно к тому же самому портативному устройству, чтобы привязать портативное устройство к множеству вычислительных устройств.

[0025] Следовательно, в соответствии с одним вариантом осуществления изобретения, концептуально показанном на Фиг.1, пользователь может осуществить сопряжение портативного устройства (например, мобильного телефона 210) и одного компьютера (например, домашнего настольного компьютера 220) вручную один раз (например, по стрелке 221), и в дальнейшем портативное устройство может автоматически привязываться к прочим компьютерам (например, компьютеру 230 класса лэптоп, как показано по стрелке 231, или офисному настольному компьютеру 240, как показано по стрелке 241), которые используются тем же самым пользователем. В качестве используемого здесь упоминания о портативном устройстве, привязываемом автоматически, означает, что пользователю компьютера и портативного устройства не требуется выполнять какие-либо действия для того, чтобы произвести аутентификацию портативного устройства компьютером или компьютера портативным устройством и способствовать их взаимной привязке.

[0026] Аспект изобретения, относящийся к предоставлению возможности автоматической привязки между портативным устройством и компьютером, в отношении которого ранее не было выполнено сопряжение с портативным устройством, может быть реализован любым приемлемым способом, так как он не ограничивается какой-либо конкретной методикой реализации. В соответствии с одним иллюстративным

вариантом осуществления настоящего изобретения, используется методика, которая может быть использована в отношении портативного устройства, выполненного с возможностью привязки к двум или более компьютерам. Создается информация аутентификации, которая аутентифицирует портативное устройство, и информация аутентификации хранится в хранилище информации, доступном для двух или более компьютеров, и так, что привязывает информацию аутентификации к пользователю портативного устройства. Как только информация аутентификации создана и сохранена в хранилище информации, доступном для компьютера, к которому портативное устройство ранее не было привязано, этот компьютер может осуществить доступ к и использовать информацию аутентификации, чтобы произвести автоматическую аутентификацию портативного устройства, не требуя операции сопряжения вручную. Это может быть достигнуто любым приемлемым способом.

[0027] Например, в соответствии с другим вариантом осуществления изобретения, когда вычислительное устройство обнаруживает по меньшей мере одно портативное устройство, которое не было к нему привязано, то вычислительное устройство может идентифицировать пользователя, вошедшего в систему вычислительного устройства, использовать информацию, идентифицирующую вошедшего в систему пользователя, чтобы получить информацию аутентификации для портативного устройства, и использовать полученную информацию аутентификации, чтобы аутентифицировать портативное устройство и автоматически привязать его к вычислительному устройству.

[0028] Как должно быть принято во внимание из вышеупомянутого, Заявители исходят из того, что недостаток обычных способов привязки портативного устройства к нескольким вычислительным устройствам состоит в том, что когда происходит обмен информацией аутентификации между портативным устройством и вычислительным устройством, информация, которая может быть использована для аутентификации портативного устройства и в дальнейшем разрешить автоматическую привязку, обычно сохраняется вычислительным устройством так, что она доступна только локально для этого вычислительного устройства. В соответствии с одним вариантом осуществления настоящего изобретения, информация аутентификации в отношении портативного устройства сохраняется таким образом, который делает ее более глобально доступной для одного или более вычислительных устройств, даже для вычислительных устройств, не использованных для осуществления связи с портативным устройством для создания информации аутентификации. В результате, в том случае, когда портативное устройство обнаруживается таким вычислительным устройством впервые, то вычислительное устройство может осуществить доступ к хранилищу информации, получить информацию аутентификации и использовать ее, чтобы аутентифицировать и автоматически привязать портативное устройство, даже когда вычислительное устройство ранее никогда не привлекалось к осуществлению сопряжения с портативным устройством вручную. Это концептуально показано на Фиг.2, при этом портативное устройство 901 может быть привязанным, в различные моменты времени, как обозначено пунктирными линиями 903a и 903b, к двум или более компьютерам 905a и 905b. Информация 909 аутентификации, которая может использоваться, чтобы аутентифицировать портативное устройство 901, хранится в хранилище 907 информации, которое доступно двум или более компьютерам 905a-b. Следовательно, когда портативное устройство 901 обнаруживается любым из компьютеров 905a-b, включая один, с которым ранее для портативного устройства 901 не было осуществлено сопряжение вручную, чтобы создать информацию аутентификации, то компьютер 905a-b может осуществить доступ к хранилищу 907 информации для получения информации 909 аутентификации и

использования ее, чтобы аутентифицировать и автоматически привязать портативное устройство 901 к компьютеру.

[0029] В конфигурации, показанной на Фиг.2, хранилище 907 информации проиллюстрировано как доступное каждому компьютеру 905a-b через сеть 911. В соответствии с одним вариантом осуществления изобретения, сеть 911 может быть любой приемлемой сетью (например, Интернет), а хранилище 907 информации может быть ассоциировано с вычислительным устройством (например, сервером базы данных или другим типом вычислительного устройства), которое отличается от любого из компьютеров 905a-b. Тем не менее, должно быть принято во внимание, что описанные здесь аспекты настоящего изобретения не ограничиваются в этом отношении. Например, хранилище 907 информации может быть предоставлено на или ассоциировано с одним из компьютеров 905a-b и может быть доступно для компьютеров 905a-b через флэш USB устройство или любую другую приемлемую среду связи.

[0030] В соответствии с одним вариантом осуществления настоящего изобретения, рассматриваемым ниже, информация 909 аутентификации становится известной посредством сопряжения вручную портативного устройства 901 с одним из компьютеров 905a-b, и затем сохраняется в хранилище 907 информации, которое может быть хранилищем информации на компьютере, который выполнял сопряжение вручную, или другом компьютере. Тем не менее, должно быть принято во внимание, что описанные здесь аспекты настоящего изобретения не ограничиваются в этом отношении, так как информация аутентификации может создаваться и сохраняться в хранилище 907 информации любым приемлемым способом. Например, в альтернативном варианте осуществления настоящего изобретения, информация аутентификации (например, ключевые материалы) может формироваться без выполнения операции сопряжения вручную. Впоследствии часть(и) ключевых материалов, которая будет использоваться портативным устройством во время автоматической привязки, может храниться непосредственно на портативном устройстве любым приемлемым образом, а часть(и) ключевых материалов, которая будет использоваться одним или более компьютерами, может храниться в глобально доступном хранилище.

[0031] Как должно приниматься во внимание из вышеупомянутого, один вариант осуществления настоящего изобретения направлен на процесс типа показанного на Фиг.3, для привязки портативного устройства к компьютеру. Исходно, на этапе 1001 производится сопряжение вручную портативного устройства с первым компьютером (например, компьютером 905a на Фиг.2), чтобы создать информацию аутентификации (например, информацию 909 аутентификации), которая может быть использована, чтобы аутентифицировать портативное устройство. Должно быть принято во внимание, что в качестве альтернативы информация аутентификации может быть создана, как упоминалось выше, другими способами. На этапе 1003 информация аутентификации сохраняется в хранилище информации (например, хранилище 907 информации), которое доступно другому компьютеру (например, компьютеру 905b), и является привязанной к пользователю портативного устройства 901. Применительно к этому, в соответствии с одним вариантом осуществления настоящего изобретения, информация аутентификации сохраняется в хранилище информации таким образом, который позволяет привязать ее к пользователю портативного устройства, чтобы компьютер, который обнаруживает портативное устройство, мог идентифицировать пользователя компьютера и использовать эту информацию, чтобы идентифицировать, какую информацию аутентификации получить из хранилища информации. Применительно к этому, в соответствии с некоторыми вариантами осуществления настоящего изобретения,

хранилище информации (например, хранилище 907 информации) может включать в себя информацию аутентификации для любого числа портативных устройств и/или любого числа из одного или более пользователей так, что когда информация в отношении многочисленных устройств пользователей сохраняется, то идентификационные данные пользователя компьютера, который обнаруживает портативное устройство, могли бы использоваться чтобы идентифицировать соответствующую информацию аутентификации для этого устройства пользователя. Тем не менее, должно быть принято во внимание, что не все варианты осуществления ограничиваются использованием информации, идентифицирующей пользователя, для идентификации того, какую информацию аутентификации использовать, чтобы аутентифицировать портативное устройство, так как может использоваться любой приемлемый метод.

[0032] На этапе 1005 компьютер, отличный от того, который производил сопряжение вручную с портативным устройством для создания информации аутентификации (например, второй компьютер, такой как компьютер 905b), может осуществить доступ к хранилищу информации, чтобы получить информацию аутентификации (например, информацию 909 аутентификации). Этот этап может выполняться в ответ на обнаружение этим компьютером портативного устройства, или в любой другой подходящий момент времени.

[0033] В итоге, на этапе 1007 компьютер может использовать полученную информацию аутентификации (например, информацию 909 аутентификации), чтобы аутентифицировать портативное устройство 901 и автоматически привязать портативное устройство к компьютеру (например, 905b), когда оно успешно прошло аутентификацию. Таким образом, портативное устройство может быть автоматически привязано к компьютеру (например, компьютеру 905b), даже не осуществляя с этим компьютером сопряжение вручную.

[0034] Как должно быть принято во внимание из вышеупомянутого, процесс, проиллюстрированный на Фиг.3, отличается от известных методик привязки портативного устройства к одному или более компьютерам как способом хранения информации аутентификации (например, в хранилище информации, доступном другим компьютерам, в противоположность только локальному использованию посредством компьютера, который выполнял операцию сопряжения вручную, чтобы получить информацию аутентификации), так и процессом, выполняемым компьютером, когда он впервые обнаруживает портативное устройство, к которому он ранее не был привязан (например, посредством получения информации аутентификации из хранилища информации в отличие от выполнения операции сопряжения вручную).

[0035] Применительно к этому, Фиг.4 иллюстрирует процесс в соответствии с одним вариантом осуществления настоящего изобретения, который задействует создание информации аутентификации для портативного устройства, которая доступна для одного или более компьютеров, которые ранее не были привязаны к портативному устройству. На этапе 1101 создается информация аутентификации, которая может использоваться для аутентификации портативного устройства. В соответствии с тем, что рассматривалось выше, информация аутентификации может быть создана посредством сопряжения вручную портативного устройства с компьютером или любым другим приемлемым способом, так как описанные здесь аспекты настоящего изобретения не ограничиваются какой-либо конкретной методикой создания информации аутентификации.

[0036] На этапе 1103 информация аутентификации сохраняется таким образом,

который делает ее доступной для множества компьютеров, в отличие от того чтобы сохранять ее локализованным образом, доступной только для одного компьютера, используя любой приемлемый метод, примеры которого здесь описаны. В соответствии с одним вариантом осуществления настоящего изобретения, информация аутентификации сохраняется таким образом, который позволяет привязать ее к пользователю портативного устройства, чтобы способствовать ее получению в соответствии с тем, как рассматривалось выше.

[0037] Фиг.5 иллюстрирует процесс, который компьютер может выполнять в соответствии с одним вариантом осуществления настоящего изобретения, чтобы автоматически привязать себя к портативному устройству. Процесс по Фиг.5 может быть инициирован в ответ на обнаружение компьютером портативного устройства или в ответ на любое приемлемое событие. На этапе 1201 процесс идентифицирует пользователя, вошедшего в систему компьютера. После этого на этапе 1203 процесс получает из хранилища информации такую информацию аутентификации, которая привязана к портативному устройству, а так же привязана к пользователю, который идентифицирован на этапе 1201 в качестве вошедшего в систему компьютера. Это может выполняться любым приемлемым способом, примеры которых рассматриваются здесь. На этапе 1205 компьютер использует информацию аутентификации, чтобы выполнить определение того, может ли портативное устройство (например, портативное устройство 901) успешно аутентифицировать себя в качестве доверенного устройства. Это может быть достигнуто любым приемлемым способом, примеры которых рассматриваются ниже. Когда на этапе 1205 определяется, что портативное устройство не может себя аутентифицировать в качестве доверенного устройства, процесс завершается, и портативное устройство не привязывается к компьютеру. В качестве альтернативы, когда на этапе 1205 определяется, что портативное устройство может успешно аутентифицировать себя в качестве доверенного устройства, процесс переходит к этапу 1207, при этом портативное устройство автоматически привязывается к компьютеру так, что никакого выполнения сопряжения вручную не требуется.

[0038] В соответствии с тем, что рассматривалось выше, информация аутентификации (например, 909 на Фиг.2), которая может храниться в хранилище информации, доступном для множества компьютеров, может иметь любой приемлемый вид. Например, информация аутентификации может содержать некоторую информацию, которая не является общедоступной (именуемую здесь для удобства как «секретная») и которую компьютер, использующий информацию аутентификации для аутентификации портативного устройства, ожидал бы, что будет иметь возможность предоставить только доверенное портативное устройство, привязанное к информации аутентификации.

[0039] В качестве альтернативы, в соответствии с другими вариантами осуществления настоящего изобретения, информация аутентификации может включать в себя один или более ключевые материалы, которые могут использоваться компьютером, который получает ключевой материал(ы), чтобы осуществлять связь с портативным устройством в соответствии с одним или более протоколами безопасности. Например, в одном не накладывающем ограничения варианте осуществления часть ключевого материала(ов) может использоваться компьютером для проверки цифровой подписи, сопровождающей сообщение, тем самым устанавливая, что сообщение было действительно передано доверенным портативным устройством, так как только доверенное портативное устройство, привязанное к информации аутентификации, должно иметь возможность отправки такого сообщения совместно с допустимой цифровой подписью. В другом примере, часть ключевого материала(ов) может использоваться компьютером, чтобы

расшифровать сообщение, которое было зашифровано портативным устройством.

[0040] В этом описании изобретения словосочетание «ключевой материал» используется для обозначения любой информации, которая может использоваться в целях обеспечения безопасности связи, например, для сохранения конфиденциальности и целостности сообщений и/или для аутентификации источников сообщений. Примеры ключевых материалов включают в себя пары открытого-закрытого ключа (используемые при шифровании с ассиметричным ключом и электронных подписях), секретные ключи (используемые при шифровании с симметричным ключом), случайные одноразовые значения (например, случайные значения, которые используются один раз, а затем игнорируются), и контрольные суммы/хэш-значения (как правило, формируемые криптографическими хэш-функциями и используемые в различных целях, таких как проверка целостности и/или привязок). Это всего лишь примеры ключевых материалов, которые могут использоваться для создания информации аутентификации, которая используется в соответствии с некоторыми описанными здесь вариантами осуществления. В дополнение, должно быть принято во внимание, что информация аутентификации, хранящаяся в хранилище информации, может воплощать в себе любую информацию, которая позволяет осуществлять к ней доступ посредством компьютера, чтобы аутентифицировать портативное устройство любым приемлемым способом, так как описанные здесь аспекты настоящего изобретения не ограничиваются использованием конкретного типа ключевого материала или прочей информации аутентификации.

[0041] В соответствии с одним вариантом осуществления настоящего изобретения, предпринимаются шаги не только чтобы аутентифицировать портативное устройство компьютером до момента предоставления возможности автоматической привязки, но и чтобы подобным же образом аутентифицировать портативным устройством компьютер и/или его пользователя до того, как портативное устройство позволит компьютеру стать автоматически привязанным к нему. Следовательно, некоторые описанные ниже варианты осуществления изобретения реализуют методики для аутентификации портативным устройством компьютера и/или его пользователя в дополнение к аутентификации компьютером портативного устройства до момента разрешения их взаимной автоматической привязки. Тем не менее, должно быть принято во внимание, что все аспекты настоящего изобретения не ограничены в этом отношении, так как описанные здесь методики могут использоваться только для аутентификации компьютером портативного устройства, чтобы в свою очередь предоставить возможность автоматической привязки.

[0042] Известные методики для автоматической привязки устройства требуют, чтобы каждый компьютер хранил отдельный набор ключевых материалов (созданных во время сопряжения вручную) для каждого портативного устройства, к которому он имеет возможность выполнить автоматическую привязку. Подобным же образом и портативное устройство обычно должно хранить обычный набор ключевых материалов (так же созданных во время сопряжения вручную) для каждого компьютера, к которому устройство может быть автоматически привязано. Это происходит потому, что в существующих методиках привязки устройства ключевые материалы, созданные в результате сопряжения вручную двух устройств, являются специфичными для устройства и привязаны к устройствам.

[0043] В качестве примера известной методики привязки, Фиг.6 показывает упрощенный вариант протокола Простого Сопряжения Bluetooth. Исходно, на этапе 310 два устройства с поддержкой Bluetooth обнаруживают друг друга, и на этапе 320

они создают незащищенный канал связи. Далее, на этапе 330 два участвующих устройства обмениваются своими открытыми ключами. На этапе 340 на основании полученных обменом открытых ключей и/или адресов Bluetooth участвующих устройств вычисляются значения подтверждения, и на этапе 350, используя адреса Bluetooth участвующих устройств, вычисляется связующий ключ для обслуживания сопряжения, который на этапе 360 используется для участия в зашифрованной связи.

[0044] Как должно быть принято во внимание из вышеупомянутого, ключевые материалы, созданные используя Простое Сопряжение Bluetooth, привязаны к адресам Bluetooth участвующих устройств. По этой причине, ключевые материалы, созданные для пары устройств, как правило, не используются повторно для привязки другой пары устройств, даже если две пары имеют одно общее устройство и/или ключевые материалы могут быть переданы от одного устройства к другому. Например, если ключевые материалы, созданные для портативного устройства и первого компьютера, имеющего первый адрес Bluetooth, были использованы при попытке привязать второй компьютер и портативное устройство, то портативное устройство отвергнет привязку ко второму компьютеру, так как ключевые материалы привязаны к первому адресу Bluetooth и портативное устройство может распознать, что второй компьютер имеет другой адрес Bluetooth. Следовательно, в соответствии с одним вариантом осуществления изобретения, используются ключевые материалы шифрования, которые не зависят от устройства и таким образом могут легко и безопасно совместно использоваться различными компьютерами в целях привязки устройства.

[0045] В одном варианте осуществления, создаются независящие от устройства ключевые материалы, через процедуру сопряжения вручную или иным образом, не между портативным устройством и каким-либо конкретным компьютером, а, наоборот, между портативным устройством и его пользователем. По этой причине, в отличие от ключевых материалов, формируемых с использованием обычных протоколов привязки устройства, ключевые материалы не привязаны к какому-либо конкретному компьютеру и поэтому могут использоваться для привязки портативного устройства к любому компьютеру или группе компьютеров. В соответствии с одним вариантом осуществления настоящего изобретения, используется такой протокол привязки, который использует независящие от устройства ключевые материалы для привязки портативного устройства к компьютеру. Тем не менее, ключевые материалы, протокол привязки и прочие описанные здесь методики не ограничиваются в этом отношении и могут использоваться для выполнения привязки между любыми двумя или более устройствами любого типа, включая не только между портативным устройством и устройством, обычно именуемым как компьютер (например, компьютер класса лэптоп или персональный компьютер), но и между любыми двумя устройствами любого типа. В дополнение, должно быть принято во внимание, что используемое здесь упоминание компьютера или вычислительного устройства (при этом понятия используются здесь взаимозаменяемо) должно относиться к любому устройству, которое имеет программируемый процессор, включая устройства, которые обычно могут не именоваться компьютером. В дополнение, описанные здесь методики могут использоваться для выполнения привязок среди групп устройств. Например, описанные здесь методики могут использоваться в сценарии широковещательной передачи или многоадресной передачи, чтобы предоставить возможность привязать группу устройств, которые совместно используют первый набор ключевых материалов, к другой группе устройств, которые совместно используют второй набор ключевых материалов.

[0046] Независящие от устройства ключевые материалы, используемые в соответствии

с одним вариантом осуществления, могут быть сделаны доступными для любого компьютера в целях привязки портативного устройства. Это может быть достигнуто любым приемлемым способом. Например, ключевые материалы могут быть сохранены на первом компьютере, к которому привязано портативное устройство, и в дальнейшем переданы второму компьютеру по запросу пользователя или в ответ на автоматический запрос от второго компьютера. В качестве альтернативы, первый компьютер может хранить ключевые материалы в глобально доступном хранилище так, что второй компьютер может получить из него ключевые материалы. Глобально доступное хранилище может находиться на первом компьютере или отдельном компьютере и/или может быть таким, поиск которого может осуществляться, используя любой приемлемый интерфейс, такой как web интерфейс, интерфейс сетевой файловой системы или любой другой приемлемый интерфейс.

[0047] В соответствии с описанным ниже одним вариантом осуществления настоящего изобретения, независящие от устройства ключевые материалы, которые будут использоваться множеством компьютеров для привязки портативного устройства, формируются, используя уникальные идентификаторы (ID) как для пользователя, так и для портативного устройства. Эти уникальные идентификаторы могут быть созданы любым приемлемым способом, так как аспекты настоящего изобретения, которые используют эти ID для формирования ключевых материалов, не ограничиваются в этом отношении. Например, уникальный ID пользователя может быть адресом электронной почты пользователя или уникальным идентификатором, предоставленным через услугу, которая предоставляет уникальные идентификаторы, такую как Windows Live ID, доступную от Microsoft Corporation, или любую другую услугу, либо может быть предоставлен любым другим приемлемым способом. Аналогично, с помощью уникального идентификатора, используя приемлемый метод, может быть идентифицировано портативное устройство, как, например, Глобально Уникальным Идентификатором (GUID) или любым другим приемлемым методом.

[0048] Обращаясь к Фиг.7, в виде схемы сообщений проиллюстрирован процесс сопряжения вручную портативного устройства и компьютера, чтобы создать независящие от устройства ключевые материалы в соответствии с одним вариантом осуществления изобретения. Процесс, проиллюстрированный на Фиг.7, может начинаться после того, как портативное устройство 410 и компьютер 420 обнаружили друг друга и создали канал связи (например, незащищенный канал) любым приемлемым способом. Например, применительно к Bluetooth, портативное устройство может быть переведено в режим разрешенного обнаружения, а компьютер 420 может произвести поиск, чтобы обнаружить портативное устройство 410, и может инициировать связь с портативным устройством 410. В зависимости от основополагающего способа связи, обмен сообщениями, проиллюстрированный на Фиг.7, может выполняться во время обнаружения и установления связи или во время любой приемлемой фазы связи между двумя участвующими устройствами, так как изобретение не ограничивается в этом отношении.

[0049] На этапе 430 компьютер 420 отправляет портативному устройству 410 первую совокупность информации, которая содержит ID пользователя (ID_{user}), открытый ключ пользователя (PK_{user}) и случайное значение, сформированное для привязки пользователя к портативному устройству 410 ($R_{user,dev}$). Случайное значение $R_{user,dev}$ является частью секретной информации, которая уникальным образом идентифицирует привязку пользователя к портативному устройству 410. Как рассматривается ниже в соответствии

с одним вариантом осуществления, $R_{user,dev}$ может использоваться для обеспечения безопасности в отношении атаки повторного воспроизведения, при которой устройство пытается неправильно себя представить, чтобы создать автоматическую привязку.

[0050] Тем не менее, должно быть принято во внимание, что аспект настоящего изобретения в отношении протокола создания независящих от устройства ключевых материалов не ограничивается использованием дополнительной части секретной информации, такой как $R_{user,dev}$, чтобы обеспечить защиту от таких атак, так как она может быть пропущена в некоторых вариантах осуществления (например, если полагают, что вероятность возникновения такой атаки минимальна). В дополнение, в то время как секретная информация в одном варианте осуществления предоставляется в виде случайного числа, должно быть принято во внимание, что для создания секретной информации может использоваться любой метод, так как он не ограничивается случайным числом.

[0051] В одном варианте осуществления, используется способ по обеспечению безопасности передачи случайного числа к портативному устройству. Это может быть выполнено любым приемлемым способом. Например, передача может осуществляться через устройство USB или по беспроводной технологии близости, такой как NFC, которая имеет настолько малую дальность передачи, которая делает практически невозможным осуществление перехвата другим устройством.

[0052] На этапе 440 портативное устройство 410 отправляет компьютеру 420 вторую совокупность информации, которая содержит ID портативного устройства 410 (ID_{dev}) и открытый ключ портативного устройства 410 (PK_{dev}).

[0053] Должно быть принято во внимание, что описанные здесь методики не ограничиваются ни дополнительным сочетанием информации, полученным путем обмена на этапах 430 и 440, ни числом и порядком сообщений, показанных на Фиг.7. Например, в одном варианте осуществления открытые ключи могут отправляться между компьютером 420 и портативным устройством 410 в сертификатах, подписанных авторитетным источником, являющимся доверенным как для портативного устройства 410, так и компьютера 420, чтобы повысить безопасность, несмотря на то, что это не требуется. Кроме того, обмен информацией может производиться любым приемлемым способом, включая разбиение этапов 430 и 440 на несколько сообщений и чередование сообщений в любом приемлемом порядке.

[0054] На этапе 450 портативное устройство 410 отображает на своем дисплее, по меньшей мере, некоторую информацию, предоставленную компьютером 420 или полученную из него, а компьютер 420 аналогично отображает на своем дисплее, по меньшей мере, некоторую информацию, принятую от портативного устройства 410, или информацию полученную из него, для того чтобы позволить пользователю подтвердить, что устройства, осуществляющие связь, являются правильными устройствами, и тем самым установить, что связь является доверенной. Отображаемая информация является информацией, которую пользователь должен иметь возможность удостоверить как предоставленную другим устройством для установления доверительного отношения. Это может быть достигнуто любым приемлемым способом, например таким, который рассматривается ниже. Например, в одном варианте осуществления портативное устройство 410 может отобразить ID_{user}, а компьютер 420 может отобразить ID_{dev}, и подобным образом пользователь может иметь возможность увидеть, какому из устройств принадлежит ID, который передается другому (например, пользователь может иметь возможность увидеть ID_{dev} на портативном устройстве 410

и ID_{user} с компьютера 420) так, что пользователь может проверить, что каждое устройство правильно отображает идентификатор, отправленный другим.

[0055] Некоторые устройства (например, портативное устройство 410) могут не иметь дисплея или интерфейса пользователя, который позволяет отображать информацию, чтобы позволить пользователю визуализировать и подтвердить ее. В соответствии с одним вариантом осуществления настоящего изобретения, для таких устройств, этап отображения информации на таком портативном устройстве может быть пропущен. Пропуск этапа может воспрепятствовать проверке пользователем того, что портативное устройство обменивается информацией с требуемым компьютером (например, 420). Тем не менее, если пользователь готов принять следующее из этого снижение безопасности, этап может быть пропущен целиком. В качестве альтернативы, в таком случае, средства связи, используемые для осуществления обмена информацией между портативным устройством и компьютером, должны быть такими, которые не оставляют сомнений в том, что связь осуществляют два доверенных устройства. Например, связь может осуществляться через проводное соединение, посредством портативного средства связи, такого как USB устройство флэш-памяти, или используя технологию связи, такую как NFC, которая имеет очень малую дальность передачи и исключает возможность перехвата или внедрения сообщения третьим вычислительным устройством.

[0056] На этапе 460 пользователь подтверждает, что сопряжение и обмен информацией происходят между доверенными устройствами, посредством взаимодействия с одним из или как с портативным устройством 410, так и компьютером 420. Например, если отображаемые на этапе 450 ID являются правильными, то пользователь может указать это посредством управления интерфейсом пользователя на портативном устройстве 410 и компьютере 420. Когда это указано, компьютер 420 и портативное устройство продолжат выполнение в соответствии с описанным ниже порядком. В качестве альтернативы, если пользователь не смог указать, что обмен информацией происходит между доверенными устройствами, процесс завершится, а информация привязки не будет сохранена.

[0057] Должно быть принято во внимание, что пользователь может быть проинформирован о предстоящем отображении информации на компьютере 420 и портативном устройстве 410 любым приемлемым способом. Например, каждое устройство (например, портативное устройство 410 и компьютер 420) может предоставить интерфейс пользователя, посредством которого оно может отобразить пользователю свой собственный ID или прочую информацию так, чтобы пользователь мог обратить внимание на информацию, ожидаемую для просмотра на другом устройстве, чтобы проверить доверительное отношение. Например, как упоминалось выше, портативное устройство может отобразить свой ID пользователю в своем собственном интерфейсе пользователя так, чтобы пользователь мог знать, какую информацию ему ожидать для отображения на компьютере 420, чтобы подтвердить, что компьютер 420 осуществляет сопряжение с правильным портативным устройством 410. Тем не менее, это всего лишь пример, так как пользователь может быть проинформирован об информации, отображение которой ожидается на одном из или обоих сопрягающихся устройствах, любым приемлемым способом.

[0058] Как рассматривалось выше, когда пользователь подтверждает, что отношение является доверенным, посредством взаимодействия с одним из или как с портативным устройством 410, так и компьютером 420, то портативное устройство 410 и компьютер 420 сохраняют, по меньшей мере, некоторую из принятой на этапах 430 и 440

информацию и/или полученную из них информацию. Например, портативное устройство 410 может сохранить профиль <ID_{user}, PK_{user}, $R_{user,dev}$> в любом внутреннем хранилище (например, памяти), доступном в портативном устройстве, в то время как компьютер 420 может сохранить профиль <ID_{dev}, PK_{dev}, $R_{user,dev}$> в глобально доступном хранилище в определенном месте, ассоциированном с пользователем. Может быть получена и сохранена в этих профилях дополнительная и/или альтернативная информация, так как описанные здесь методики не ограничиваются какой-либо конкретной информацией, полученной путем обмена. Так же могут использоваться другие приемлемые типы информации. Иллюстративный пример способа, которым профиль, созданный на Фиг.7, может использоваться для аутентификации портативного устройства одним или более компьютерами (включая компьютеры, отличные от компьютера 420) и обеспечения автоматической привязки, описывается ниже

[0059] Фиг.8 иллюстрирует характерную конфигурацию глобально доступного хранилища 801 информации для хранения профилей устройств, созданных для множества пользователей (с пользователя 1 до пользователя N), используя протокол и информацию, проиллюстрированные на Фиг.7. Как упоминалось выше, эти профили являются всего лишь иллюстративными, так что глобально доступное хранилище информации может быть организовано другими способами, чтобы хранить другие типы информации. В варианте осуществления, проиллюстрированном на Фиг.8, каждый пользователь имеет возможность быть привязанным к множеству устройств. Например, информация, хранящаяся и привязанная к пользователю 1, включает в себя три записи 805a-c, каждая из которых соответствует различным устройствам, привязанным к пользователю 1. Например, записи 805a-c могут соответствовать мобильному телефону, проигрывателю MP3 и комплекту беспроводных наушников, при этом все из перечисленного принадлежит одному и тому же пользователю, хотя это всего лишь примеры, так как портативное устройство(а), привязанное к пользователю, может быть любым приемлемым портативным устройством(ами).

[0060] Должно быть принято во внимание, что одно и то же портативное устройство может совместно использоваться несколькими пользователями. По этой причине, в соответствии с одним вариантом осуществления изобретения, проиллюстрированным на Фиг.8, одно и то же устройство может быть привязано в хранилище 801 информации к нескольким пользователям. Это показано, например, посредством того, что устройство, идентифицируемое идентификатором ID_{dev1}, привязано к пользователю 1 посредством записи 805a и дополнительно привязано к пользователю 2 посредством записи 807a.

[0061] Как может быть видно на Фиг.8 в соответствии с одним вариантом осуществления, записи 805a и 807a не идентичны, так как значения, которые идентифицируют привязки между пользователями и портативным устройством, являются разными (т.е., $R_{user1,dev1}$, и $R_{user2,dev1}$).

[0062] Использование отличающихся значений, которые идентифицируют привязки между конкретным пользователем и конкретным устройством, может применяться в соответствии с одним вариантом осуществления настоящего изобретения, чтобы обеспечить защиту от потенциальных атак повторного воспроизведения со стороны пользователя без доверия. В этом отношении, должно быть принято во внимание, что описанные здесь методики могут использоваться применительно к компьютерам и прочим устройствам, которые могут совместно использоваться несколькими пользователями. Следовательно, в соответствии с одним вариантом осуществления

настоящего изобретения, использование уникального значения, идентифицирующего привязку между пользователем и портативным устройством, может применяться для предотвращения атак повторного воспроизведения, организуемых пользователем без доверия. Такие атаки могут иметь какой-либо или несколько видов. Например, как должно быть принято во внимание из вышеупомянутого, в процессе обмена информацией аутентификации между компьютером и конкретным портативным устройством (в этом примере именуемым как устройство 1), устройство 1 примет информацию, которую компьютер отправляет, чтобы произвести аутентификацию идентификационных данных пользователя, вошедшего в систему компьютера (например, ID_{user}, подписанный ключом, привязанным к пользователю). Следовательно, эта информация может быть сохранена на портативном устройстве (например, в этом примере на устройстве 1). Если другой пользователь получил управление над этим портативным устройством (например, устройством 1), то существует опасность того, что пользователь может заставить устройство повторно воспроизвести информацию, полученную от компьютера, и тем самым портативное устройство может, по сути, сымитировать, что оно является компьютером с вошедшим в его систему первым пользователем (например, пользователем 1), и произвести поиск автоматической привязки к другому устройству (например, устройству 2) как пользователь 1, в то время как на самом деле портативное устройство находится под управлением другого пользователя (например, пользователя 2).

[0063] Должно быть принято во внимание, что подобная опасность существует и когда компьютер, вовлеченный в обмен информацией для аутентификации портативного устройства, примет информацию, которую портативное устройство использует для аутентификации себя самого (например, уникальный идентификатор для портативного устройства, подписанный ключом портативного устройства), и эта информация может быть сохранена на компьютере и потенциально повторно воспроизведена компьютером, чтобы сымитировать идентификационные данные портативного устройства во время поиска с целью сформировать привязку к другому компьютеру или другому типу устройства, в систему которого вошел пользователь отличный от пользователя 1 (например, пользователь 2). Например, в процессе обмена информацией аутентификации между компьютером и устройством 1, компьютер примет информацию, которую устройство 1 отправляет, чтобы аутентифицировать себя самого (например, ID_{dev} подписанный ключом, привязанным к dev1). Следовательно, эта информация может быть сохранена на компьютере. Если злонамеренный субъект может заставить этот компьютер повторно воспроизвести информацию, принятую от устройства 1, то тем самым компьютер может, по сути, сымитировать, что он является устройством 1 и произвести поиски автоматической привязки с другим пользователем (например, пользователем 2) как устройство 1.

[0064] В соответствии с одним вариантом осуществления настоящего изобретения, включение в информацию идентификации, обмен которой происходит между устройствами, значения, которое уникально идентифицирует привязку между конкретным пользователем и конкретным устройством, предотвращает тип атаки повторного воспроизведения, рассмотренный выше. Например, применительно к устройству, чтобы правильно аутентифицировать сообщение, принятое от компьютера, на котором предположительно имеется конкретный вошедший в его систему пользователь, устройство произведет проверку, чтобы убедиться в том, что оно принимает конкретное уникальное значение, идентифицирующее привязку между ним (т.е. конкретным устройством) и пользователем. Вследствие этого, так как устройство,

принимающее информацию аутентификации от компьютера, имеет всю информацию, которая ему требуется, чтобы аутентифицировать идентификационные данные пользователя, вошедшего в систему компьютера, то оно не принимает информацию, которая может потребоваться другому устройству, чтобы аутентифицировать пользователя, так как каждое устройство имеет свое собственное уникальное значение, относящееся к привязке между ним самим и пользователем. Вследствие этого, устройство, принимающее информацию аутентификации от пользователя (например, устройство 1 в примере выше), не может успешно сымитировать идентификационные данные компьютера, на котором имеется вошедший в его систему пользователь, чтобы привязаться к другому устройству (например, устройству 2 в примере выше), так как устройство, предпринимающее такую атаку повторного воспроизведения, не обладает конкретным значением, которое ожидает принять другое устройство (например, устройство 2), чтобы аутентифицировать идентификационные данные пользователя.

[0065] Аналогично, использование значения, которое конкретно идентифицирует привязку между конкретным пользователем и конкретным устройством, может использоваться, чтобы защитить компьютер, который принял информацию аутентификации от любого устройства (например, устройства 1) для привязки к вошедшему в систему пользователю, от попыток сымитировать идентификационные данные этого устройства и сформировать привязку к другому компьютеру или другому устройству, в систему которого вошел другой пользователь. Например, применительно к компьютеру, чтобы правильно аутентифицировать сообщение, принятое от портативного устройства, предположительно привязанного к пользователю, вошедшему в систему компьютера, компьютер произведет проверку, чтобы убедиться в том, что он принимает конкретное уникальное значение, идентифицирующее привязку между портативным устройством и пользователем, вошедшим в систему компьютера. Вследствие этого, так как компьютер, принимающий информацию аутентификации от портативного устройства, чтобы привязать ее к первому пользователю, имеет всю информацию, которая ему требуется для аутентификации идентификационных данных портативного устройства с первым пользователем, то он не принимает информацию, которая требуется для представления, чтобы аутентифицировать портативное устройство со вторым пользователем, так как каждый пользователь имеет уникальное значение, относящееся к привязке между каждым пользователем и портативным устройством. Вследствие этого, компьютер, принимающий информацию аутентификации от портативного устройства (например, устройства 1 в примере выше), чтобы привязать ее к первому пользователю (например, пользователю 1 в примере выше), не может успешно сымитировать идентификационные данные устройства 1, чтобы привязаться к другому компьютеру, имеющему другого вошедшего в его систему пользователя (например, пользователь 2 в примере выше), так как компьютер, предпринимающий такую атаку повторного воспроизведения, не обладает конкретным значением, которое будет ожидать принять другой пользователь (например, пользователь 2), чтобы аутентифицировать идентификационные данные портативного устройства.

[0066] В одном варианте осуществления, значения, уникально идентифицирующие привязки, хранятся в одном или более безопасных и защищенных от подделки местоположениях. В качестве альтернативы, значения могут храниться в зашифрованном виде, при этом ключи расшифровки хранятся в одном или более безопасных и защищенных от подделки местоположениях.

[0067] Дополнительно должно быть принято во внимание, что в глобально доступном хранилище могут храниться другие типы информации вместо или в дополнение к

описанным выше профилям. Например, в глобально доступном хранилище могут храниться открытые и секретные ключи, которые используются в протоколе, показанном на Фиг.11. Тем не менее, это не является обязательным, так как пользователь может получить открытый и секретный ключи из других местоположений памяти, например, из локального местоположения памяти на компьютере, в систему которого вошел пользователь.

[0068] Фиг.9 иллюстрирует характерную конфигурацию памяти портативного устройства, которая содержит множество профилей 903a-b, созданных для пользователей портативного устройства. Несмотря на то, что на Фиг.9 показаны только два профиля 903a-b, должно быть принято во внимание, что может храниться любое приемлемое число профилей. Каждый профиль может соответствовать отдельному пользователю портативного устройства, или пользователь может определить несколько профилей для использования в различных ситуациях так, чтобы один и тот же человек мог быть распознан системой в качестве разных пользователей (например, посредством разных ID пользователя). В характерном сценарии пользователь может использовать ID_{user1}, чтобы войти в систему одного или более домашних компьютеров, и ID_{user2}, чтобы войти в систему одного или более рабочих компьютеров. Хранение обоих профилей на портативном устройстве, один для ID_{user1}, а другой для ID_{user2}, позволяет портативному устройству осуществлять автоматическую привязку к любому компьютеру, в систему которого вошел пользователь, используя один из двух ID пользователя. Должно быть принято во внимание, что изобретение не ограничивается числом пользователей, которые могут быть одновременно привязаны к портативному устройству. В некоторых вариантах осуществления, портативное устройство может разрешать привязку только к одному пользователю за раз, в то время как в других вариантах осуществления портативные устройства могут разрешать привязки к более чем одному пользователю за раз (например, портативное устройство может иметь верхнее ограничение по числу пользователей, к которым одновременно может быть привязано портативное устройство).

[0069] Вновь должно быть принято во внимание, что в памяти портативного устройства могут храниться другие типы информации вместо или в дополнение к профилям, показанным на Фиг.9. Например, могут храниться открытый и секретный ключи портативного устройства, которые используются в протоколе, показанном на Фиг.11.

[0070] Как только профили созданы и сохранены в портативном устройстве и глобально доступном хранилище информации (используемое здесь упоминание хранилища информации, которое глобально доступно, означает, что хранилище информации не привязано к одному компьютеру и может быть доступно для двух и более различных компьютеров), то информация, содержащаяся на нем, может использоваться для взаимной аутентификации портативного устройства и компьютера и способствовать автоматической привязке, используя любой приемлемый метод, примеры которых рассматриваются ниже. Тем не менее, должно быть принято во внимание, что информация профиля (или любой другой тип секретных или ключевых материалов, который может использоваться в целях аутентификации, как рассматривается выше) может быть образована способами, отличными от использования процесса сопряжения вручную по Фиг.7. Например, как рассматривалось выше, в соответствии с одним вариантом осуществления настоящего изобретения, секретная информация может быть создана, не прибегая к операции сопряжения вручную

портативного устройства и какого-либо компьютера. Характерный процесс этого типа показан на Фиг.10 для использования с конкретными профилями, рассмотренными выше применительно к Фиг.8 и 9. Тем не менее, должно быть принято во внимание, что аспект настоящего изобретения, который позволяет создание ключевых материалов без сопряжения вручную, не ограничивается использованием с конкретными типами ключевых материалов, включенными в профили, показанные на Фиг.8 и 9.

[0071] В процессе по Фиг.10 на этапе 710 получают для пользователя и портативного устройства ключевые материалы, которые включают в себя пару открытого-закрытого ключей и случайное значение. Пары открытого-закрытого ключей и случайные числа могут быть вновь сформированными на этапе 710 или могут быть получены ранее существовавшие открытый-закрытый ключи и значения случайного числа. Для получения ключевых материалов может использоваться любое приемлемое вычислительное устройство(а), так как изобретение не ограничивается в этом отношении.

[0072] На этапе 720 часть(и) ключевых материалов, которая должна быть сохранена на портативном устройстве, передается портативному устройству любым приемлемым способом (например, от компьютера, который имеет ключевые материалы и осуществляет их передачу портативному устройству через проводное или беспроводное соединение, через носитель, читаемый портативным компьютером, который может быть подсоединен к портативному устройству для загрузки с него ключевой информации и т.д.). Сохраненная информация может включать в себя информацию, которую портативное устройство предоставляет компьютеру, чтобы произвести свою аутентификацию (например, ID_{dev}, PK_{dev} и $R_{user,dev}$), закрытый ключ (например, SK_{dev}) для устройства, который образует пару открытого-закрытого ключей с открытым ключом, передаваемым компьютерам, к которым устройство может быть автоматически привязано, и, для каждого пользователя портативного устройства, информацию, которая, как ожидается, будет передана от компьютера к портативному устройству, чтобы разрешить портативному устройству аутентифицировать компьютер или его пользователя (например, ID_{user}, PK_{user}, $R_{user,dev}$).

[0073] На этапе 730 информация, используемая компьютером для аутентификации портативного устройства и разрешения автоматической привязки, сохраняется в глобально доступном хранилище информации и привязывается к пользователю (например, как показано на Фиг.8). Следовательно, в варианте осуществления, показанном на Фиг.8, профиль устройства $<ID_{dev}, PK_{dev}, R_{user,dev}>$ сохраняется для каждого устройства, привязанного к пользователю.

[0074] Должно быть принято во внимание, что этапы 710, 720 и 730 могут выполняться в любом логическом порядке следования, и каждый может быть разбит на несколько этапов, и эти этапы могут чередоваться или выполняться в любом логическом порядке следования. В дополнение, как рассматривалось выше, конкретная проиллюстрированная на Фиг.8 ключевая информация является всего лишь иллюстративной, так как могут использоваться прочие варианты осуществления настоящего изобретения, которые используют отличную ключевую информацию.

[0075] Фиг.11 иллюстрирует характерный протокол, посредством которого компьютер и портативное устройство, которые ранее не были сопряжены вручную, могут аутентифицировать друг друга, чтобы установить доверительное отношение, которое способствует автоматической привязке в соответствии с одним вариантом осуществления изобретения. В частности, успешно осуществив протокол по Фиг.11, портативное устройство 810 докажет компьютеру 820, что портативное устройство

810 фактически является устройством, которое и подразумевается (т.е. устройством, идентифицируемым посредством идентификатора ID_{dev}), и компьютер 820 удостоверится в том, что соединение с устройством, идентифицируемым посредством $ID_{dev,}$ принято пользователем, идентифицируемым посредством ID_{user}. В дополнение, компьютер 820 докажет портативному устройству, что компьютер 820 используется пользователем, идентифицируемым посредством ID_{user}, и портативное устройство 810 удостоверится в том, что пользователь, идентифицируемый посредством ID_{user}, находится среди пользователей, для которых портативное устройство 810 принимает автоматические соединения.

[0076] Применительно к процессу, проиллюстрированному на Фиг.7, протокол по Фиг.11 может выполняться после того, как портативное устройство 810 и компьютер 820 обнаружили друг друга и создали канал связи любым приемлемым способом. Тем не менее, должно быть принято во внимание, что передача сообщений, проиллюстрированная на Фиг.11, может выполняться во время обнаружения и установления связи или во время любой приемлемой фазы связи между портативным устройством 810 и компьютером 820, так как вариант осуществления, проиллюстрированный на Фиг.11, не ограничивается в этом отношении.

[0077] Фиг.11 иллюстрирует характерный протокол, который могут использовать портативное устройство 810 и компьютер 820, чтобы аутентифицировать друг друга, используя типы ранее созданных профилей, проиллюстрированные на Фиг.8-9. Должно быть принято во внимание, что настоящее изобретение не ограничивается использованием типов профилей, проиллюстрированных на Фиг.8-9, чтобы разрешить взаимную аутентификацию между компьютером и портативным устройством, так как любые приемлемые типы профилей могут использоваться, чтобы произвести аутентификацию компьютером портативного устройства и/или портативным устройством компьютера. Более того, протокол по Фиг.11 приводит к созданию ключа, совместно используемого портативным устройством 810 и компьютером 820. Этот совместно используемый ключ может непосредственно или опосредованно использоваться, чтобы получить ключ симметричного шифрования для шифрования и расшифровки сообщений между портативным устройством 810 и компьютером 820. Тем не менее, изобретение не ограничивается созданием какого-либо конкретного ключевого материала для обеспечения защищенной связи, если было установлено доверительное отношение, или даже для использования в системах, которые не защищают сообщения, если доверительное отношение установлено.

[0078] На этапе 830 компьютер 820 уведомляет портативное устройство 810 об идентификационных данных пользователя, к которому должно быть привязано портативное устройство 810 (например, на основании идентификационных данных пользователя, вошедшего в систему компьютера 820). На этапе 840 портативное устройство 810 использует информацию, идентифицирующую пользователя (например, ID_{user}), принятую на этапе 830, чтобы получить (например, из его памяти) профиль, который портативное устройство хранит для этого пользователя и который включает в себя, в показанном примере, PK_{user} и $R_{user,dev}$. Если профиль, привязанный к ID_{user}, не может быть обнаружен, тем самым указывая на то, что портативное устройство на текущий момент не приняло соединение с пользователем, идентифицируемым посредством ID_{user}, то портативное устройство 810 может отклонить соединение, например, посредством завершения протокола. В качестве альтернативы, портативное

устройство может инициировать процедуру сопряжения вручную (не показана). Если профиль для пользователя может быть обнаружен, то из профиля получают информацию так, чтобы она могла использоваться совместно с секретным ключом портативного устройства 810, чтобы на этапе 850 предоставить компьютеру 820 обратно секретную информацию, чтобы, как рассматривается ниже, аутентифицировать портативное устройство 810. В дополнение, в варианте осуществления, проиллюстрированном на Фиг.11, полученная информация включает в себя информацию, которая позволяет портативному устройству 810 аналогично аутентифицировать компьютер 820 способом, рассматриваемым ниже.

[0079] В проиллюстрированном варианте осуществления, на этапе 840 получают секретный ключ SK_{dev} портативного устройства 810. Тем не менее, изобретение не ограничивается моментом времени, в который получают секретный ключ SK_{dev}. Например, секретный ключ SK_{dev} может быть получен до момента приема ID_{user} от компьютера 820. Аналогичным образом, новый ключ K_{dev} (использование которого рассматривается ниже) в проиллюстрированном варианте осуществления формируется на этапе 840, но он также может формироваться перед этапом 840, так как изобретение не ограничивается в этом отношении.

[0080] На этапе 850 портативное устройство 810, используя SK_{dev}, электронным образом подписывает ID_{dev}, чтобы получить первую подпись (обозначенную на Фиг.11 $sign_{SKdev}(ID_{dev})$), и собирает первое сообщение, которое содержит: первую подпись, $R_{user,dev}$, ID_{dev} и K_{dev}. Затем, используя PK_{user}, первое сообщение шифруется и отправляется компьютеру 820. Шифрование выполняется таким образом, что только субъект, обладающий SK_{user} (т.е. секретным ключом, соответствующим PK_{user}), может осуществить доступ к содержимому первого сообщения. Это предотвращает возможность перехвата содержимого первого сообщения, включая первую подпись, любым другим компьютером, находящимся в пределах дальности передачи. Может быть желательным предотвратить возможность перехвата первой подписи сторонним объектом, так как сторонний объект может позже использовать первую подпись, чтобы «выдать себя» за портативное устройство 810.

[0081] На этапе 860 компьютер 820 формирует новый ключ K_{user} (использование которого описывается ниже) и получает SK_{user}. Вновь эти два этапа могут выполняться в любом порядке и могут выполняться до этапа 860, так как изобретение не ограничивается в этом отношении. Компьютер 820 расшифровывает, используя SK_{user}, зашифрованное первое сообщение. Если фактически пользователь намерен принять первое сообщение (т.е., портативное устройство 810 ожидает привязки к пользователю, идентифицируемому посредством ID_{user}, и портативное устройство 810 использует $PK_{user,}$ чтобы зашифровать первое сообщение так, что только устройство, обладающее SK_{user}, может его расшифровать), то следует расшифровка, и компьютер 820 может извлечь из первого сообщения ID_{dev}. В качестве альтернативы, ID_{dev} может быть получен посредством некоторых других способов, например, через ранее произведенный обмен информацией между портативным устройством 810 и компьютером 820. Используя $ID_{dev,}$ компьютер может получить из глобально доступного хранилища профиль <ID_{dev}, PK_{dev}, $R_{user,dev}$> из местоположения, ассоциированного с пользователем, идентифицируемым посредством ID_{user}, так что информация, содержащаяся в

полученном профиле, может использоваться для удостоверения в том, что портативное устройство 810 является устройством, которое и подразумевается (т.е. устройством, идентифицируемым посредством идентификатора ID_{dev}), а соединение с устройством, идентифицируемым посредством ID_{dev}, является принятым пользователем, идентифицируемым посредством ID_{user}.

[0082] В одном варианте осуществления может потребоваться, чтобы компьютер 820 был аутентифицирован глобально доступным хранилищем для доступа к созданным профилям устройства для пользователя, идентифицируемого посредством ID_{user}. Например, может потребоваться, чтобы компьютер 820 представил глобально доступному хранилищу некоторые аккредитивы (credentials) пользователя, которые могут быть получены компьютером 820 автоматически в момент, когда пользователь, идентифицируемый посредством ID_{user}, входит в систему компьютера 820. В качестве альтернативы, пользователь, идентифицируемый посредством ID_{user}, может предоставить требуемые аккредитивы в некоторый момент после входа в систему.

[0083] Если профиль, привязанный к ID_{dev} и ID_{user}, не может быть обнаружен в глобально доступном хранилище, тем самым указывая на то, что пользователь, идентифицируемый посредством ID_{user}, на текущий момент не принял автоматическое соединение с портативным устройством 810, то компьютер 820 может отклонить соединение, например, посредством завершения протокола. В качестве альтернативы, компьютер 820 может инициировать процедуру сопряжения вручную (не показана).

[0084] Если профиль устройства $<ID_{dev}, PK_{dev}, R_{user,dev}>$ может быть обнаружен в глобально доступном хранилище, то компьютер 820 получает профиль и извлекает из него PK_{dev}. Затем он извлекает первую подпись из первого сообщения и проверяет первую подпись, используя PK_{dev}. Алгоритм подписи, используемый для формирования первой подписи, создан таким образом, что подпись признается действительной, используя открытый ключ, только если она была сформирована, используя секретный ключ, соответствующий открытому ключу. В проиллюстрированном варианте осуществления только субъект, обладающий SK_{dev}, может сформировать подпись, которая признается действительной в соответствии с PK_{dev}. Таким образом, портативное устройство 810 подтверждает компьютеру, что портативное устройство 810 фактически является устройством, которое подразумевается (т.е. устройством, идентифицируемым посредством идентификатора ID_{dev}).

[0085] Для того чтобы предотвратить атаки повторного воспроизведения, как рассматривалось выше, компьютер 820 так же может проверить, совпадает ли случайное значение, принятое в сообщении, со значением $R_{user,dev}$, полученным из глобально доступного хранилища.

[0086] Следовательно, если первая подпись является действительной, а значение $R_{user,dev}$ верным, то затем компьютер 820 доверяет портативному устройству 810 и переходит к вычислению совместно используемого ключа в виде $K_{dev}+K_{user}$ по причинам, рассматриваемым ниже. В противном случае компьютер 820 может отклонить соединение, например, посредством завершения протокола. Кроме того, если первая подпись действительна, компьютер 820 цифровым образом подписывает ID_{user}, используя SK_{user}, чтобы сформировать вторую подпись и может собрать второе сообщение, которое содержит вторую подпись (обозначенную на Фиг.11 как $sign_{SKuser}(ID_{user})$),

$R_{user,dev}$, ID_{user} и K_{user}. Затем второе сообщение, используя PK_{dev}, шифруется и на этапе 870 отправляется портативному устройству 810. Вновь шифрование выполняется так, чтобы только субъект, обладающий SK_{dev}, мог осуществить доступ к содержимому второго сообщения. В противном случае, любой компьютер, находящийся в пределах дальности передачи, может перехватить содержимое второго сообщения, включая вторую подпись. Может быть желательным предотвратить возможность перехвата второй подписи сторонним объектом, так как сторонний объект может позже использовать вторую подпись для того, чтобы «выдать себя» за пользователя, идентифицируемого посредством ID_{user}.

[0087] На этапе 880 портативное устройство 810, используя SK_{dev}, расшифровывает зашифрованное второе сообщение. Затем портативное устройство 810 извлекает вторую подпись из второго сообщения и проверяет вторую подпись, используя PK_{user}. Так же портативное устройство 810 проверяет, совпадает ли случайное значение, принятое в сообщении, со значением $R_{user,dev}$, полученным из памяти. Если подпись действительна, а значение $R_{user,dev}$ верно, то затем портативное устройство 810 доверяет компьютеру 820 как авторизованному пользователем, идентифицируемым посредством ID_{user}, так как только субъект, обладающий SK_{user}, мог сформировать подпись, которая является действительной при проверке, используя PK_{user}, и имеет верное полученное значение $R_{user,dev}$. В противном случае, портативное устройство может отклонить соединение, например, посредством завершения протокола.

[0088] Как должно быть принято во внимание из вышеупомянутого, тем самым протокол по Фиг.11 обеспечивает портативному устройству 810 и компьютеру 820 возможность взаимно аутентифицировать друг друга и установить доверительное отношение, даже если два устройства никогда ранее не сопрягались вручную. Впоследствии два устройства могут быть вовлечены в доверительную связь любым требуемым образом, так как описанные здесь аспекты настоящего изобретения не ограничиваются в этом отношении. В соответствии с вариантом осуществления, проиллюстрированным на Фиг.11, новые ключи K_{dev} и K_{user} были созданы в соответствии с рассмотренным выше. В соответствии с одним вариантом осуществления, когда вторая подпись и значение $R_{user,dev}$ действительны, портативное устройство 810 вычисляет совместно используемый ключ как $K_{dev}+K_{user}$. В этот момент как компьютер 820, так и портативное устройство 810 правильно вычислили Kdev+Kuser в качестве совместно используемого ключа, который в свою очередь может использоваться, чтобы получить ключи шифрования для обеспечения безопасности канала связи между портативным устройством 810 и компьютером 820. Тем не менее, должно быть принято во внимание, что описанные здесь аспекты настоящего изобретения не ограничиваются созданием совместно используемого ключа только таким образом, так как безопасность связи между компьютером 820 и портативным устройством 810 может быть обеспечена любым приемлемым способом, или не обеспечена, так как описанные здесь аспекты настоящего ограничения не ограничиваются в этом отношении.

[0089] Должно быть принято во внимание, что протокол, проиллюстрированный на Фиг.11, может выполняться портативным устройством 810 и компьютером 820 автоматически без вмешательства пользователя. Например, компьютер 820 может выполнять этап 830 автоматически в момент обнаружения портативного устройства 810 и установления канала связи с портативным устройством 810. Этап 860 так же

может выполняться автоматически, если у компьютера 820 есть доступ к аккредитивам, используемым для приема профилей устройства от глобально доступного хранилища.

[0090] Кроме того, этапы 830-880 могут выполняться в любом приемлемом порядке, включая разбиение на множественные этапы и чередование множественных этапов в любом приемлемом порядке.

[0091] Как рассматривалось выше, описанные здесь аспекты настоящего изобретения могут использоваться применительно к любому компьютеру или устройству, которое имеет процессор, который может быть запрограммирован для выполнения любых описанных выше действий. Фиг.12 является схематической иллюстрацией характерного компьютера 1300, на котором могут быть реализованы аспекты настоящего изобретения. Компьютер 1300 включает в себя процессор или модуль 1301 обработки данных и память 1302, которая может включать в себя как временную, так и постоянную память. Компьютер 1300 так же включает в себя, в дополнение к системной памяти 1302, хранилище (например, съемное хранилище 1304 и несъемное хранилище 1305). Память 1302 может хранить одну или более инструкций для того, чтобы программировать модуль 1301 обработки для выполнения любой из описанных здесь функций. Как указывалось выше, упоминание здесь компьютера может включать в себя любое устройство, которое имеет программируемый процессор, включая компьютер, смонтированный в стойке, настольный компьютер, компьютер класса лэптоп, планшетный компьютер или любое из многочисленных устройств, которые, как правило, могут не рассматриваться в качестве компьютера, но которые включают в себя программируемый процессор (например, PDA, проигрыватель MP3, мобильный телефон, беспроводные наушники и т.д.).

[0092] Так же компьютер может иметь одно или более устройств ввода и вывода, такие как устройства 1306-1307, проиллюстрированные на Фиг.13. Эти устройства могут, среди прочего, использоваться для представления интерфейса пользователя. Примеры устройств вывода, которые могут использоваться для предоставления интерфейса пользователя, включают в себя принтеры или экраны дисплея для визуального представления выходных данных и громкоговорители или другие устройства, формирующие звук для слышимого представления выходных данных. Примеры устройств ввода, которые могут использоваться применительно к интерфейсу пользователя, включают в себя клавиатуры и указательные устройства, такие как манипуляторы типа мышь, сенсорные панели и цифровые планшеты. В качестве другого примера, компьютер может принимать входную информацию посредством распознавания речи или в другом слышимом формате.

[0093] Описанные выше варианты осуществления настоящего изобретения могут быть реализованы любыми многочисленными способами. Например, варианты осуществления могут быть реализованы, используя аппаратное обеспечение, программное обеспечение или их сочетание. При реализации в программном обеспечении, код программного обеспечения может исполняться любым приемлемым процессором или совокупностью процессоров, независимо от того, будут ли они предоставлены на одном компьютере или распределены среди многочисленных компьютеров.

[0094] Дополнительно, должно быть принято во внимание, что очерченные здесь различные способы и процессы могут быть закодированы в качестве программного обеспечения, которое является исполняемым одним или более процессорами, которые используют любую одну из многообразия операционных систем или платформ. В дополнение, такое программное обеспечение может быть написано, используя любой

из числа приемлемых языков программирования и/или инструментов программирования или создания сценариев и так же может быть скомпилировано в качестве машинного кода или промежуточного кода, который исполняется на интегрированном пакете программ или виртуальной машиной.

[0095] Применительно к этому, некоторые описанные здесь аспекты изобретения могут быть воплощены в качестве машиночитаемого носителя (или нескольких машиночитаемых носителей) (например, памяти компьютера, одном или более гибких дисках, компакт-дисках, оптических дисках, магнитных лентах, элементах флэш-памяти, конфигурациях схем в Программируемых Вентильных Матрицах или других полупроводниковых устройствах или прочих материальных компьютерных носителях данных) с закодированными на них одной или более программами, которые при исполнении одним или более процессорами, выполняют способы, которые реализуют различные рассмотренные выше варианты осуществления изобретения. Машиночитаемый носитель или носители могут быть переносными, так что программа или программы, хранящиеся на них, могут быть загружены на один или более разных компьютеров или других процессоров для того, чтобы реализовать как рассматривалось выше различные аспекты настоящего изобретения.

[0096] Используемые здесь понятия «программа» или «программное обеспечение» в общем смысле относятся к любому типу компьютерного кода или набору исполняемых компьютером инструкций, которые могут использоваться для того, чтобы программировать компьютер или процессор, чтобы в свою очередь реализовать, как рассматривается выше, различные аспекты настоящего изобретения, и могут включать в себя любой микрокод компьютерной программы и т.д. В дополнение, должно быть принято во внимание, что одна или более компьютерных программ, которые при исполнении выполняют способы настоящего изобретения, не обязательно должны размещаться на одном компьютере или процессоре, а могут быть распределены между несколькими различными компьютерами или процессорами для того чтобы реализовать различные аспекты настоящего изобретения.

[0097] Исполняемые компьютером инструкции могут быть представлены в различных видах, таких как модули программы, исполняемые одним или более компьютерами или прочими устройствами. Модули программы могут включать в себя подпрограммы, программы, объекты, компоненты, структуры данных и т.д., которые выполняют конкретные задачи или реализуют конкретные типы абстрактных данных. Функциональные возможности модулей программы могут объединяться или распределяться в соответствии с тем, что требуется в различных вариантах осуществления.

[0098] Так же структуры данных могут храниться на машиночитаемом носителе в любом приемлемом виде. Для простоты иллюстрации, структуры данных могут быть показаны как имеющие поля, которые соотносятся с ячейками в структуре данных. Такие взаимосвязи так же могут быть получены посредством присвоения хранилища для полей к ячейкам на машиночитаемом носителе, который передает взаимосвязь между полями. Тем не менее, для того чтобы создать взаимосвязь между информацией в полях структуры данных может использоваться любой приемлемый механизм, включая посредством использования указателей, ярлыков или прочих механизмов, которые создают взаимосвязь между элементами данных.

[0099] Различные аспекты настоящего изобретения могут использоваться отдельно, в сочетании или в любой приемлемой компоновке или сочетании, включая те, что не были конкретно рассмотрены в вышеизложенном. Например, аспекты, описанные в

одном варианте осуществления, могут быть объединены любым образом с аспектами, описанными в другом варианте осуществления.

[0100] Само по себе использование числительных, таких как «первый», «второй», «третий» и т.д., в формуле изобретения, чтобы определить элемент формулы изобретения, не подразумевает какой-либо приоритет, превосходство или порядок одного элемента формулы изобретения над другим или порядок с привязкой по времени, в котором выполняются этапы способа, а используются всего лишь в качестве обозначений, чтобы отличать один элемент формулы изобретения, который имеет определенное название, от другого элемента, который имеет точно такое же название (но при использовании числительных), чтобы различать элементы формулы изобретения.

[0101] Так же используемая здесь фразеология и терминология служит в целях описания и не должна рассматриваться как ограничивающая. Использование здесь «включающий», «содержащий» или «имеющий», «содержащий в себе», «вовлекающий» и их вариации подразумевает охват элементов, перечисляемых впоследствии и их эквивалентов, как впрочем, и дополнительных элементов.

[0102] Следовательно, описав таким образом несколько аспектов по меньшей мере одного варианта осуществления данного изобретения, должно быть принято во внимание, что различные изменения, модификации и улучшения будут без труда приходить в голову специалисту в соответствующей области техники. Подразумевается, что такие изменения, модификации и улучшения рассматриваются внутри объема изобретения. Соответственно, вышеупомянутое описание и чертежи должны рассматриваться как предоставленные только в качестве примера.

Формула изобретения

1. Машиночитаемый носитель данных, на котором закодировано множество инструкций, которыми при их исполнении по меньшей мере одним компьютером выполняется способ аутентификации по меньшей мере одним компьютером портативного устройства, содержащий этапы, на которых:

(A) идентифицируют идентификационные данные пользователя, вошедшего в систему по меньшей мере одного компьютера;

(B) принимают на по меньшей мере одном компьютере по меньшей мере одно первое сообщение от портативного устройства, причем по меньшей мере одно первое сообщение содержит идентификатор портативного устройства и первую защищенную информацию аутентификации;

(C) используют, посредством по меньшей мере одного компьютера, идентификационные данные пользователя, вошедшего в систему по меньшей мере одного компьютера, и идентификатор портативного устройства, чтобы получить по меньшей мере один первый ключевой материал; и

(D) определяют, аутентифицирует ли по меньшей мере одно первое сообщение портативное устройство, посредством использования по меньшей мере одного первого ключевого материала, чтобы обработать первую защищенную информацию аутентификации.

2. Машиночитаемый носитель данных по п.1, в котором первая информация аутентификации содержит цифровую подпись, и по меньшей мере один первый ключевой материал содержит открытый ключ портативного устройства, при этом при определении того, аутентифицирует ли по меньшей мере одно первое сообщение портативное устройство, используют открытый ключ портативного устройства для проверки того, была ли цифровая подпись сформирована с использованием секретного ключа,

соответствующего открытому ключу портативного устройства.

3. Машиночитаемый носитель данных по п.1, при этом пользователь является первым пользователем, а портативное устройство является первым портативным устройством, и при этом:

по меньшей мере одно первое сообщение дополнительно содержит по меньшей мере один идентификатор, который предположительно идентифицирует пару, состоящую из конкретного пользователя и конкретного портативного устройства; и

при определении того, аутентифицирует ли по меньшей мере одно первое сообщение портативное устройство, определяют, уникально ли идентифицирует упомянутый по меньшей мере один идентификатор пару, которая содержит первого пользователя и первое портативное устройство.

4. Машиночитаемый носитель данных по п.1, в котором способ дополнительно содержит этапы, на которых:

создают по меньшей мере один ключ, совместно используемый по меньшей мере одним компьютером и портативным устройством, когда на этапе (D) портативное устройство определено как прошедшее аутентификацию; и

шифруют по меньшей мере одно дополнительное сообщение между по меньшей мере одним компьютером и портативным устройством, используя один или более ключей, сформированных, по меньшей мере частично, на основе этого по меньшей мере одного совместно используемого ключа.

5. Машиночитаемый носитель данных по п.4, в котором упомянутый по меньшей мере один совместно используемый ключ вычисляется посредством объединения первого ключа, к которому по меньшей мере одним компьютером осуществлен доступ и который передан в портативное устройство, и второго ключа, переданного портативным устройством в по меньшей мере один компьютер.

6. Машиночитаемый носитель данных по п.1, в котором способ дополнительно содержит этап, на котором, до приема первой защищенной информации аутентификации, отправляют в портативное устройство по меньшей мере одно предварительное сообщение, которое идентифицирует пользователя, вошедшего в систему по меньшей мере одного компьютера.

7. Машиночитаемый носитель данных по п.1, в котором способ дополнительно содержит этап, на котором передают с по меньшей мере одного компьютера в портативное устройство по меньшей мере одно второе сообщение, которое содержит вторую защищенную информацию аутентификации, которая должна быть обработана портативным устройством, чтобы определить, аутентифицирует ли по меньшей мере одно второе сообщение по меньшей мере один компьютер, причем вторая информация аутентификации должна обрабатываться портативным устройством путем использования по меньшей мере одного второго ключевого материала, хранящегося на портативном устройстве.

8. Машиночитаемый носитель данных по п.7, при этом по меньшей мере одно второе сообщение дополнительно содержит по меньшей мере один идентификатор, который уникально идентифицирует пару, состоящую из пользователя и портативного устройства.

9. Портативное устройство, которое содержит:

по меньшей мере один процессор, который запрограммирован:

принимать от компьютера по меньшей мере одно первое сообщение, идентифицирующее идентификационные данные пользователя, вошедшего в систему компьютера;

получать первый ключевой материал, при этом первый ключевой материал привязан

ко второму ключевому материалу, который доступен компьютеру и привязан к пользователю; и

передавать компьютеру по меньшей мере одно второе сообщение, причем по меньшей мере одно второе сообщение содержит идентификатор портативного устройства, причем по меньшей мере одно второе сообщение дополнительно содержит по меньшей мере одну первую порцию информации, защищенную посредством первого ключевого материала, так что компьютер может определить, аутентифицирует ли по меньшей мере одно второе сообщение портативное устройство, посредством использования второго ключевого материала, чтобы обработать по меньшей мере одну первую порцию информации, защищенную посредством первого ключевого материала.

10. Портативное устройство по п.9, в котором по меньшей мере один процессор дополнительно запрограммирован:

использовать идентификационные данные пользователя, чтобы дополнительно получить по меньшей мере один идентификатор, который уникально идентифицирует пару, которая состоит из пользователя и портативного устройства; и

передавать компьютеру этот по меньшей мере один идентификатор и/или информацию, сформированную, по меньшей мере частично, используя данный по меньшей мере один идентификатор.

11. Портативное устройство по п.9, в котором по меньшей мере один процессор дополнительно запрограммирован:

принимать от компьютера по меньшей мере одно третье сообщение, которое содержит по меньшей мере одну вторую порцию информации, защищенную посредством третьего ключевого материала, при этом третий ключевой материал привязан к четвертому ключевому материалу, который хранится на портативном устройстве; и

определять, аутентифицирует ли по меньшей мере одно третье сообщение компьютер, посредством использования четвертого ключевого материала, чтобы обработать по меньшей мере одну вторую порцию информации, защищенную посредством третьего ключевого материала.

12. Портативное устройство по п.11, при этом пользователь является первым пользователем, а портативное устройство является первым портативным устройством, и при этом:

по меньшей мере одно третье сообщение дополнительно содержит по меньшей мере один идентификатор, который предположительно идентифицирует пару, состоящую из конкретного пользователя и конкретного портативного устройства; и

определение того, аутентифицирует ли по меньшей мере одно третье сообщение компьютер, содержит определение того, уникально ли идентифицирует этот по меньшей мере один идентификатор пару, которая содержит первого пользователя и первое портативное устройство.

13. Портативное устройство по п.9, в котором первый ключевой материал является секретным ключом портативного устройства, при этом по меньшей мере один процессор запрограммирован защищать по меньшей мере одну первую порцию информации посредством цифровой подписи по меньшей мере одной первой порции информации секретным ключом портативного устройства, и при этом второй ключевой материал является открытым ключом портативного устройства.

14. Портативное устройство по п.11, в котором по меньшей мере один процессор дополнительно запрограммирован:

вычислять по меньшей мере один совместно используемый ключ, который совместно используется компьютером и портативным устройством, когда определено, что по

меньшей мере одно третье сообщение аутентифицирует компьютер; и

шифровать по меньшей мере одно дополнительное сообщение, передаваемое в компьютер, используя один или более ключей, сформированных, по меньшей мере частично, на основе этого по меньшей мере одного совместно используемого ключа.

15. Портативное устройство по п.14, в котором упомянутый по меньшей мере один совместно используемый ключ вычисляется посредством объединения первого ключа, сформированного компьютером и переданного в портативное устройство, и второго ключа, сформированного портативным устройством и переданного в компьютер.

16. Способ взаимной аутентификации портативного устройства и компьютера, которые ранее не были связаны вручную, содержащий этапы, на которых:

(A) идентифицируют посредством компьютера идентификационные данные пользователя, вошедшего в систему компьютера;

(B) передают с компьютера в портативное устройство информацию, идентифицирующую идентификационные данные пользователя, вошедшего в систему компьютера;

(C) извлекают на портативном устройстве первый ключевой материл, причем первый ключевой материал привязан ко второму ключевому материалу, который является доступным для компьютера и привязан к пользователю;

(D) передают с портативного устройства в компьютер по меньшей мере одно первое сообщение, причем по меньшей мере одно первое сообщение содержит информацию, идентифицирующую идентификационные данные портативного устройства, при этом по меньшей мере одно первое сообщение дополнительно содержит по меньшей мере одну первую порцию информации, защищенную посредством первого ключевого материала;

(E) определяют на компьютере, аутентифицирует ли по меньшей мере одно первое сообщение портативное устройство, путем использования второго ключевого материала для обработки по меньшей мере одной первой порции информации, защищенной посредством первого ключевого материала;

(F) используют на компьютере идентификационные данные портативного устройства, чтобы извлечь из хранилища данных, которое не является эксклюзивным для компьютера, третий ключевой материал, причем третий ключевой материал привязан к четвертому ключевому материалу, который хранится на портативном устройстве;

(G) передают с компьютера в портативное устройство по меньшей мере одно второе сообщение, содержащее по меньшей мере одну вторую порцию информации, защищенную посредством третьего ключевого материала; и

(H) определяют на портативном устройстве, аутентифицирует ли по меньшей мере одно второе сообщение компьютер, путем использования четвертого ключевого материала для обработки по меньшей мере одной второй порции информации, защищенной посредством третьего ключевого материала.

17. Способ по п.16, в котором первый ключевой материал представляет собой секретный ключ портативного устройства, при этом по меньшей мере одну первую порцию информации защищают посредством цифровой подписи по меньшей мере одной первой порции информации секретным ключом портативного устройства, при этом второй ключевой материал представляет собой открытый ключ портативного устройства.

18. Способ по п.16, в котором пользователь является первым пользователем, а портативное устройство является первым портативным устройством, при этом:

по меньшей мере одно первое сообщение дополнительно содержит по меньшей мере

один идентификатор, который предположительно идентифицирует пару, состоящую из конкретного пользователя и конкретного портативного устройства; и

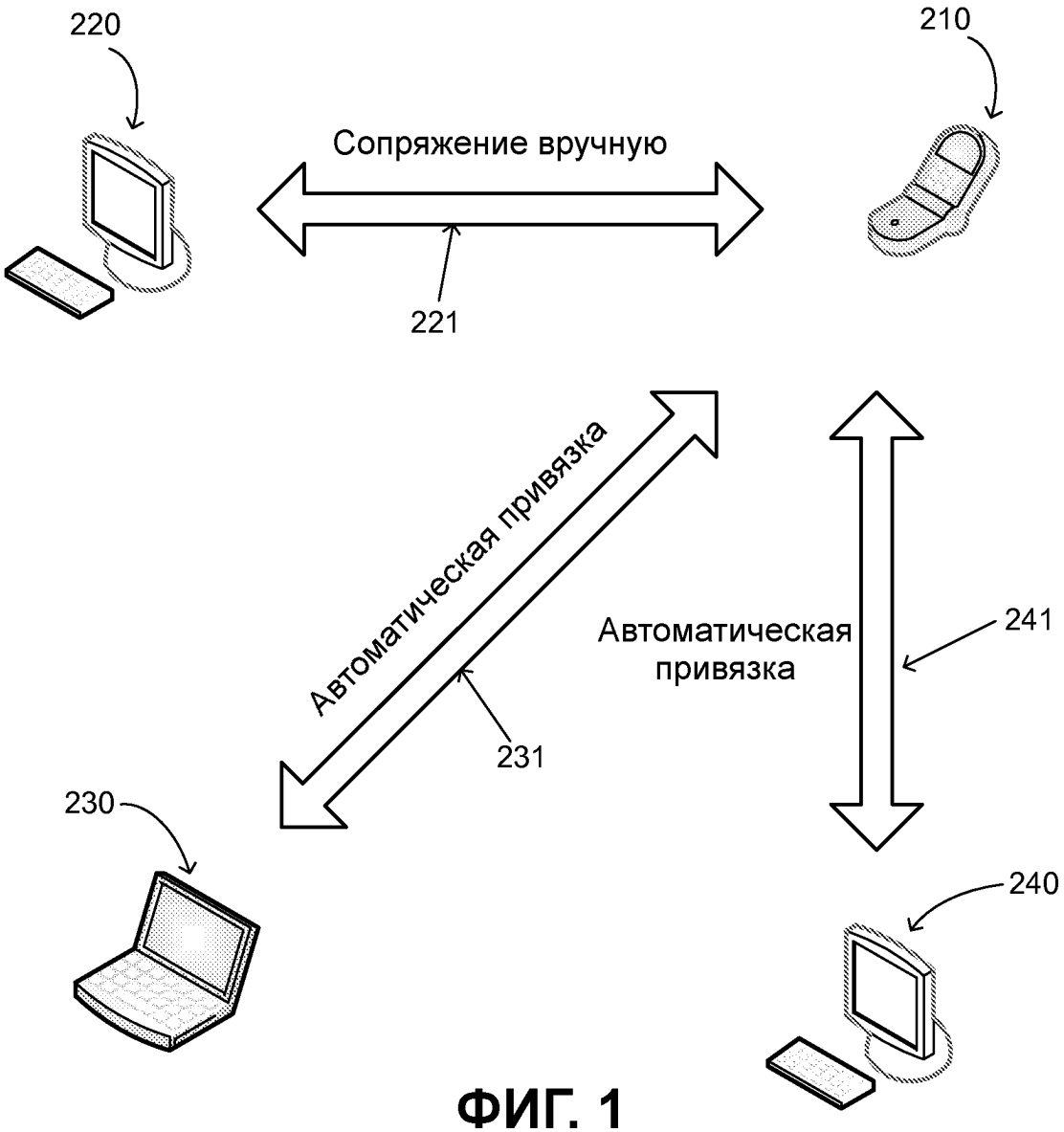
при определении того, аутентифицирует ли по меньшей мере одно первое сообщение портативное устройство, определяют, уникально ли идентифицирует этот по меньшей мере один идентификатор пару, которая содержит первого пользователя и первое портативное устройство.

19. Способ по п.16, в котором третий ключевой материал представляет собой секретный ключ пользователя, и по меньшей мере одну вторую порцию информации защищают посредством цифровой подписи по меньшей мере одной второй порции информации секретным ключом пользователя, при этом четвертый ключевой материал представляет собой открытый ключ пользователя.

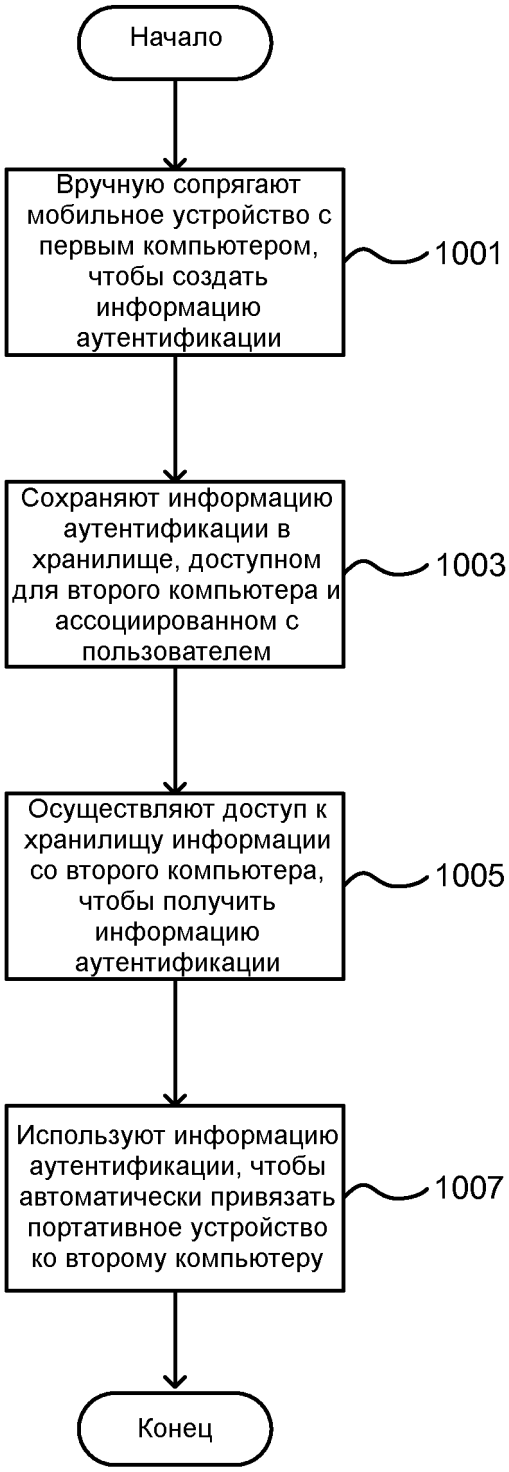
20. Способ по п.16, в котором пользователь является первым пользователем, а портативное устройство является первым портативным устройством, при этом:

по меньшей мере одно второе сообщение дополнительно содержит по меньшей мере один идентификатор, который предположительно идентифицирует пару, состоящую из конкретного пользователя и конкретного портативного устройства; и

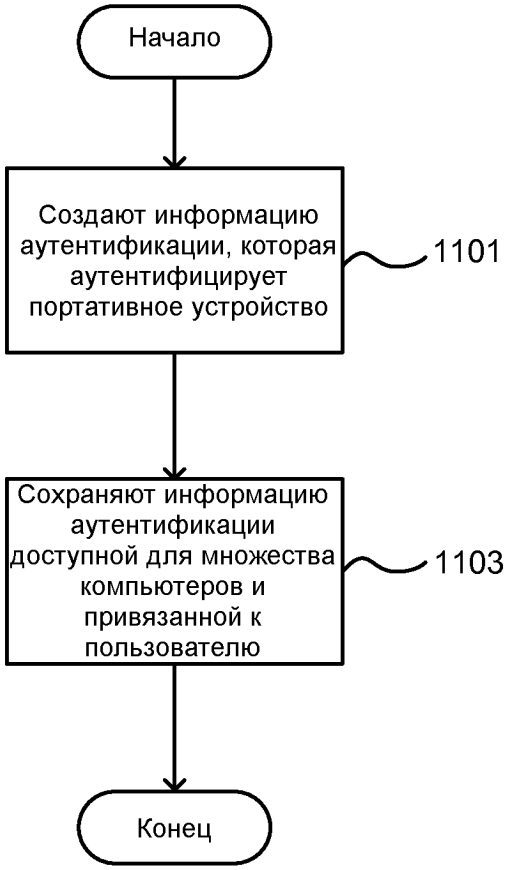
при определении того, аутентифицирует ли по меньшей мере одно второе сообщение компьютер, определяют, является ли пользователь, вошедший в систему компьютера, первым пользователем, посредством определения того, уникально ли идентифицирует этот по меньшей мере один идентификатор пару, которая содержит первого пользователя и первое портативное устройство.


220
210
Сопряжение вручную
221
Автоматическая привязка
231
Автоматическая
привязка
241
230
240

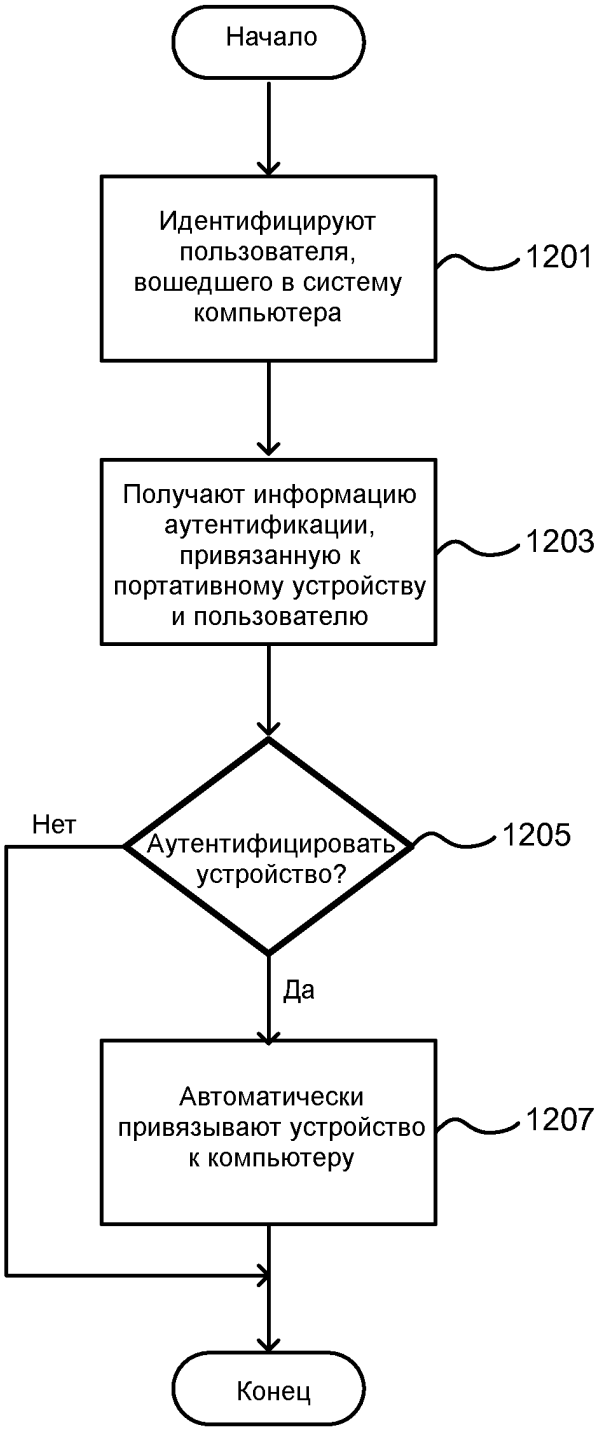
ФИГ. 1


Начало
Вручную сопрягают мобильное устройство с первым компьютером, чтобы создать информацию аутентификации
1001
Сохраняют информацию аутентификации в хранилище, доступном для второго компьютера и ассоциированном с пользователем
1003
Осуществляют доступ к хранилищу информации со второго компьютера, чтобы получить информацию аутентификации
1005
Используют информацию аутентификации, чтобы автоматически привязать портативное устройство ко второму компьютеру
1007
Конец

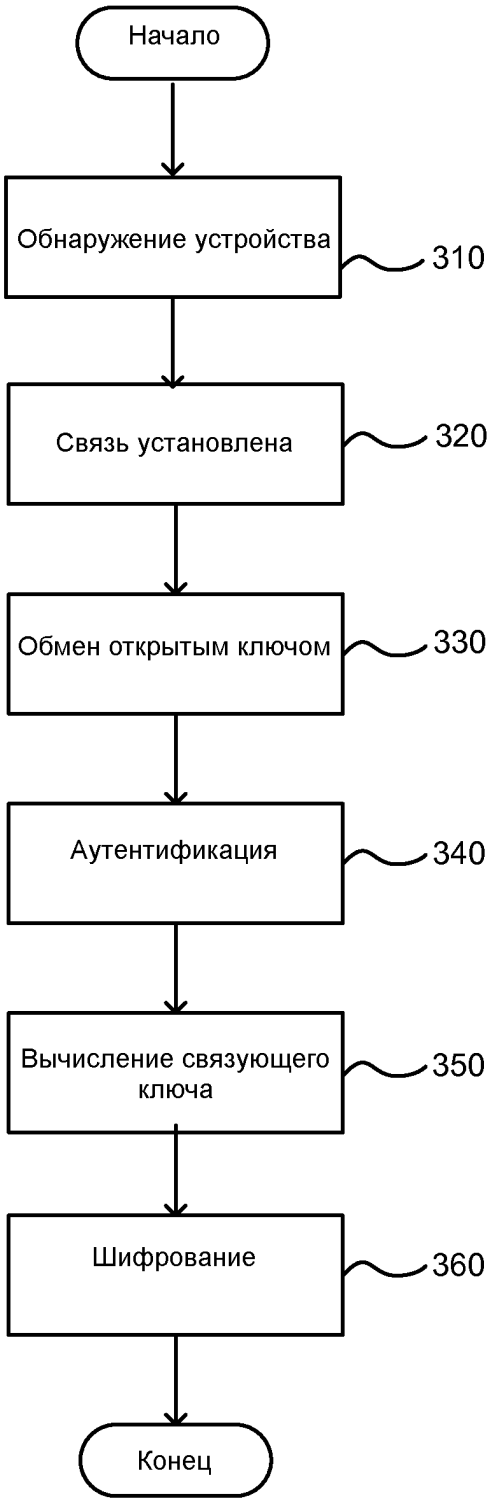
ФИГ. 3


Начало
Создают информацию аутентификации, которая аутентифицирует портативное устройство
1101
Сохраняют информацию аутентификации доступной для множества компьютеров и привязанной к пользователю
1103
Конец

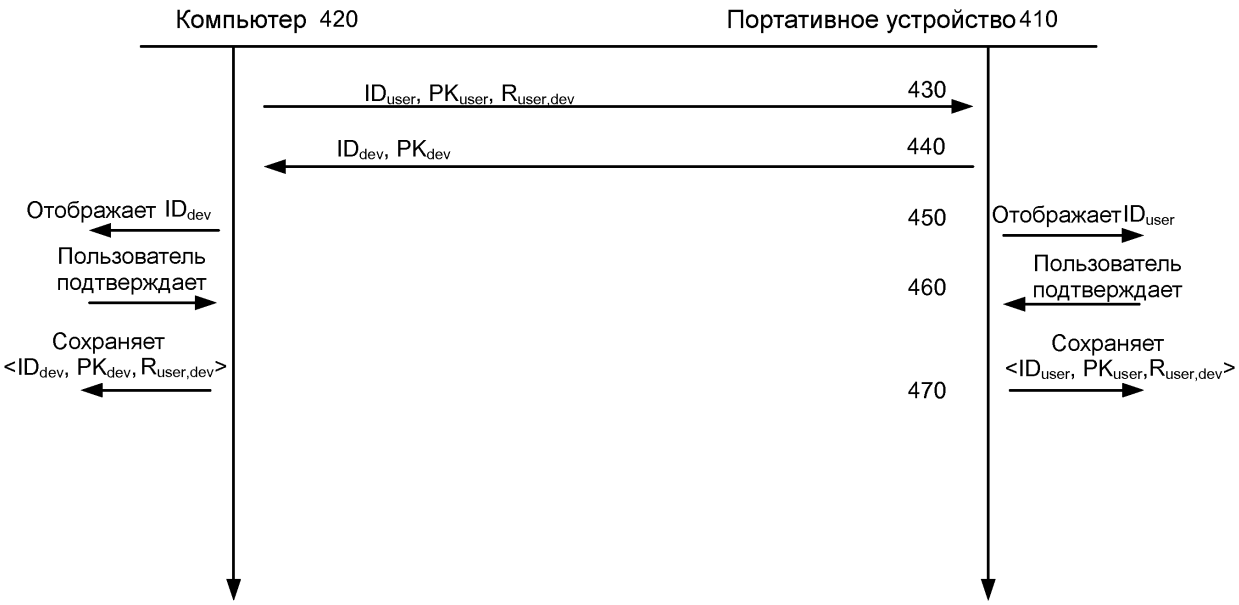
ФИГ. 4


Начало
Идентифицируют пользователя, вошедшего в систему компьютера
1201
Получают информацию аутентификации, привязанную к портативному устройству и пользователю
1203
Аутентифицировать устройство?
1205
Нет
Да
Автоматически привязывают устройство к компьютеру
1207
Конец

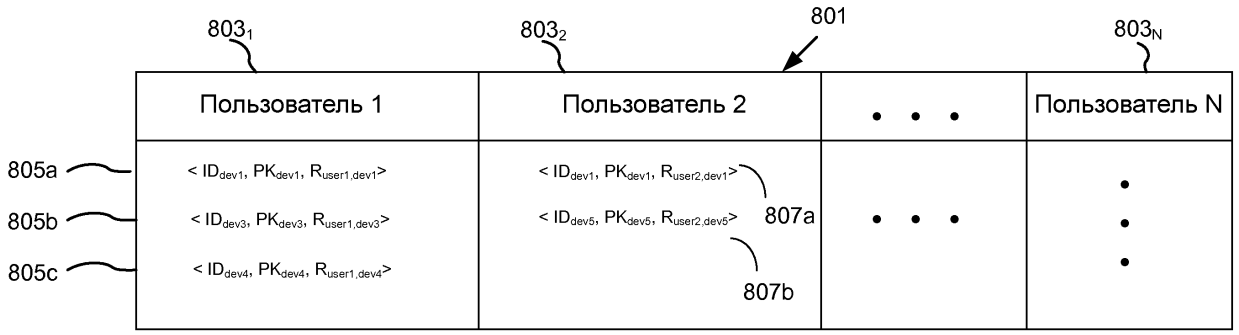
ФИГ. 5


Начало
Обнаружение устройства
310
Связь установлена
320
Обмен открытым ключом
330
Аутентификация
340
Вычисление связующего ключа
350
Шифрование
360
Конец

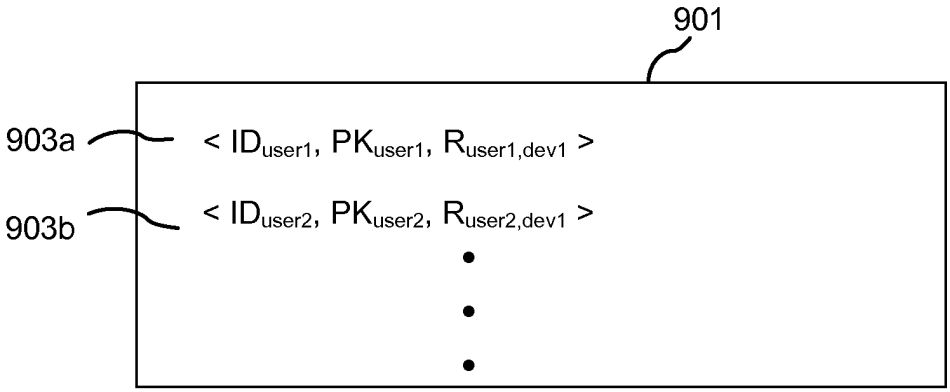
ФИГ. 6



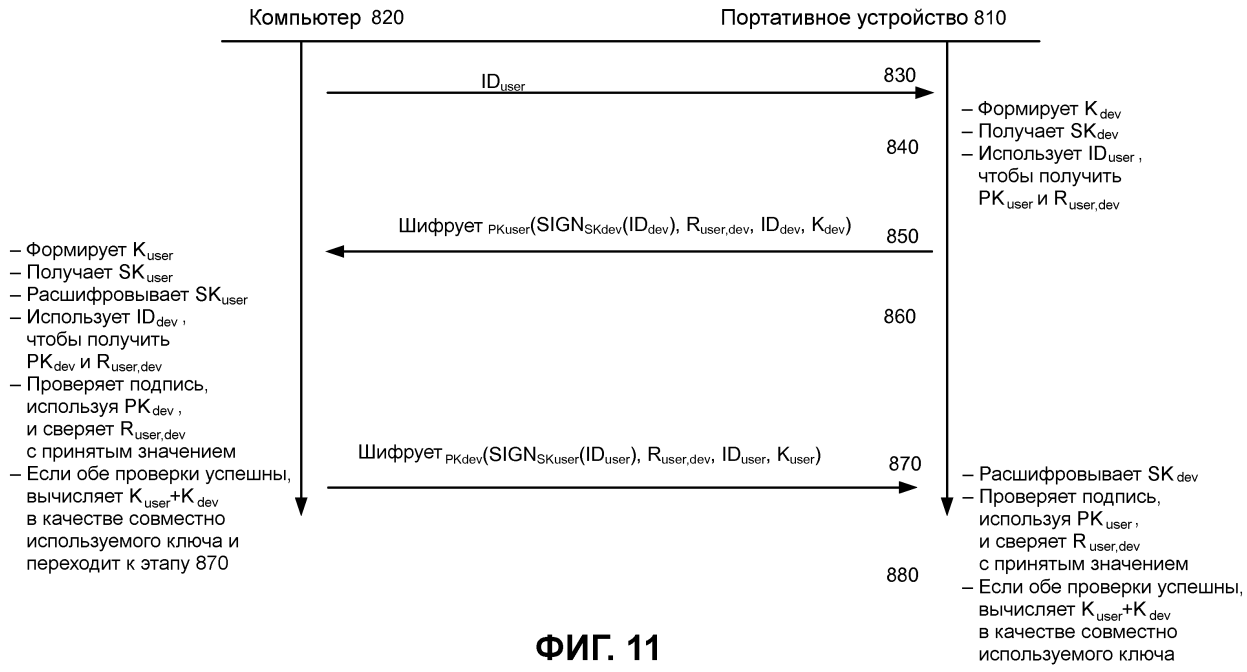
ФИГ. 7



ФИГ. 8



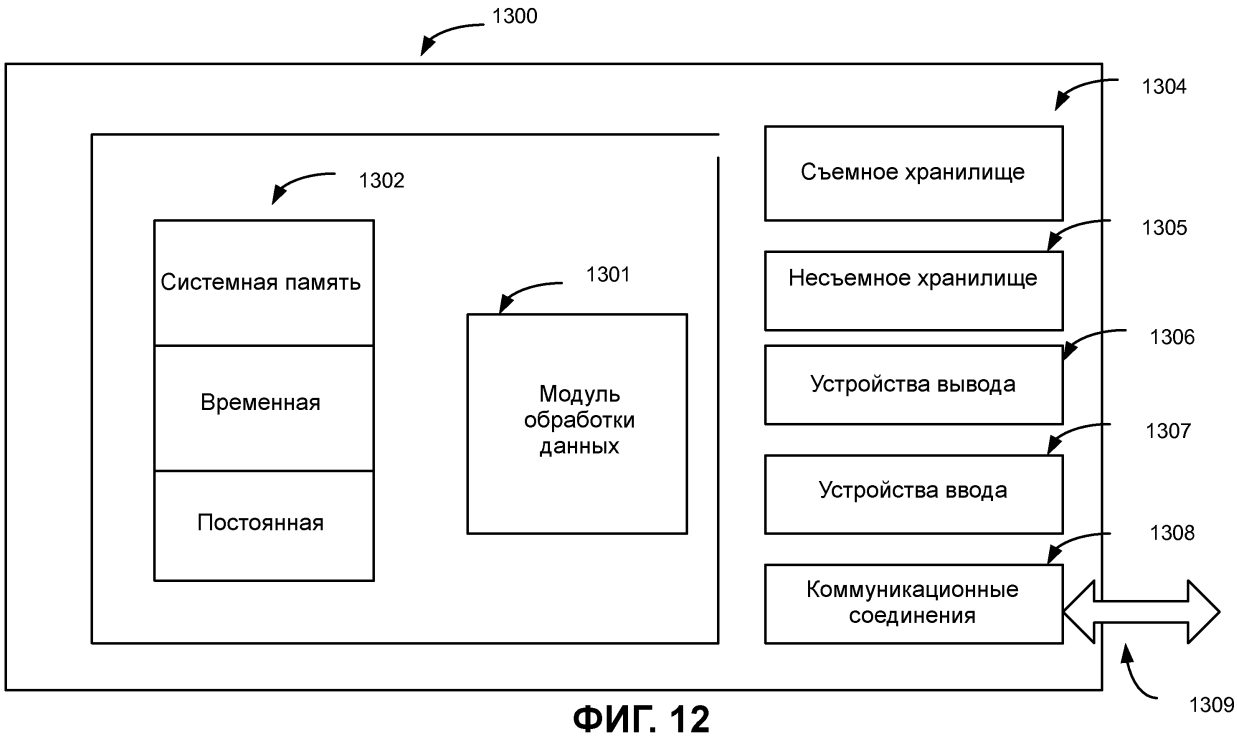
ФИГ. 9



ФИГ. 11

Компьютер 820
Портативное устройство 810
ID_{user}
830
– Формирует K_{dev}
– Получает SK_{dev}
– Использует ID_{user}, чтобы получить PK_{user} и $R_{user,dev}$
840
Шифрует $_{PKuser}(SIGN_{SKdev}(ID_{dev}), R_{user,dev}, ID_{dev}, K_{dev})$
850
– Формирует K_{user}
– Получает SK_{user}
– Расшифровывает SK_{user}
– Использует ID_{dev}, чтобы получить PK_{dev} и $R_{user,dev}$
– Проверяет подпись, используя PK_{dev}, и сверяет $R_{user,dev}$ с принятым значением
– Если обе проверки успешны, вычисляет $K_{user}+K_{dev}$ в качестве совместно используемого ключа и переходит к этапу 870
860
Шифрует $_{PKdev}(SIGN_{SKuser}(ID_{user}), R_{user,dev}, ID_{user}, K_{user})$
870
– Расшифровывает SK_{dev}
– Проверяет подпись, используя PK_{user}, и сверяет $R_{user,dev}$ с принятым значением
– Если обе проверки успешны, вычисляет $K_{user}+K_{dev}$ в качестве совместно используемого ключа
880

ФИГ. 11


1300
1304
Съемное хранилище
1305
Несъемное хранилище
1306
Устройства вывода
1307
Устройства ввода
1308
Коммуникационные соединения
1309
1302
Системная память
Временная
Постоянная
1301
Модуль обработки данных

ФИГ. 12