РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 702 076**(13) **C2**

(51) МПК
*H04L 9/32* (2006.01)
*G06F 21/33* (2013.01)
*G06F 21/32* (2013.01)
*H04W 12/06* (2009.01)

# (12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
*H04L 9/3231 (2013.01); H04L 63/0823 (2013.01); G06F 21/31 (2013.01); H04W 12/06 (2013.01)*

(21)(22) Заявка: **2017140260, 23.04.2015**

(24) Дата начала отсчета срока действия патента:
**23.04.2015**

Дата регистрации:
**03.10.2019**

Приоритет(ы):
(22) Дата подачи заявки: **23.04.2015**

(43) Дата публикации заявки: **23.05.2019** Бюл. № **15**

(45) Опубликовано: **03.10.2019** Бюл. № **28**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **23.11.2017**

(86) Заявка PCT:
**KR 2015/004048 (23.04.2015)**

(87) Публикация заявки PCT:
**WO 2016/171295 (27.10.2016)**

Адрес для переписки:
**191002, Санкт-Петербург, а/я 5, Общество с ограниченной ответственностью "Ляпунов и партнеры"**

(72) Автор(ы):
**ЧХОИ Унхо (KR)**

(73) Патентообладатель(и):
**ЧХОИ Унхо (KR)**

(56) Список документов, цитированных в отчете о поиске: **US 2012/0278614 A1, 01.11.2012. US 2010/0185864 A1, 22.07.2010. US 2014/0101453 A1, 10.04.2014. RU 2452013 C2, 27.05.2012.**

## (54) АУТЕНТИФИКАЦИЯ В РАСПРЕДЕЛЕННОЙ СРЕДЕ

(57) Реферат:

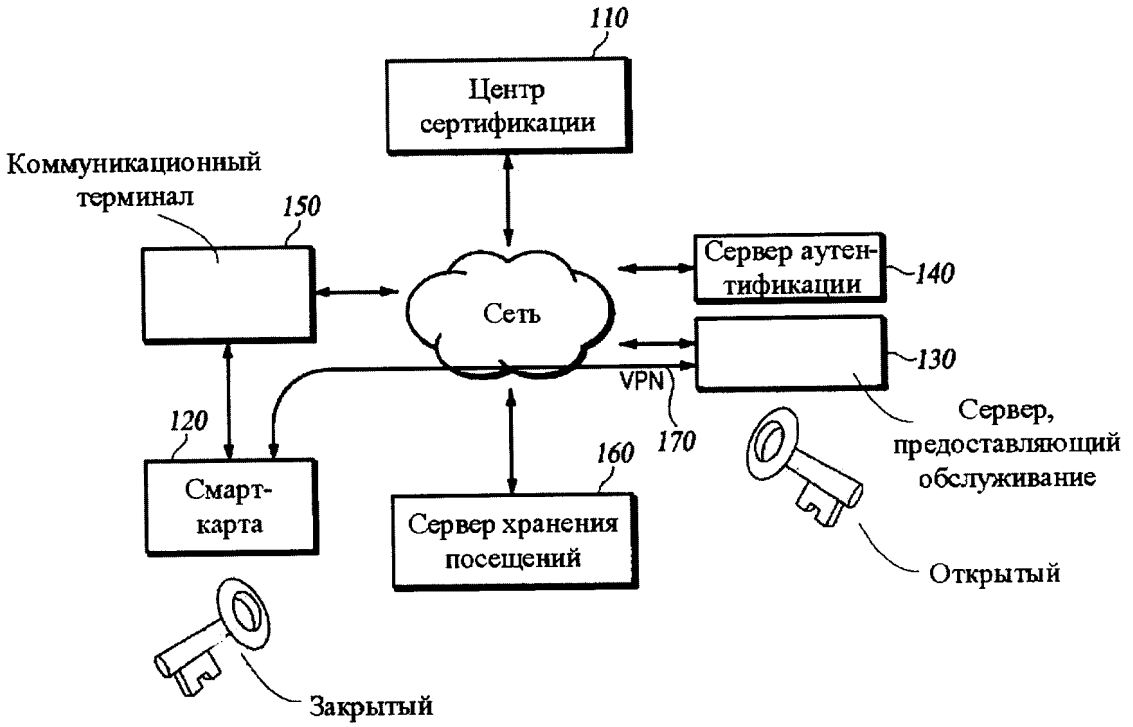
Изобретение относится к области вычислительной техники. Технический результат заключается в повышении информационной безопасности удаленного подключения вычислительной системы. Технический результат достигается за счет сбора посредством портативного устройства биометрических данных или комбинации фрагментов биометрических данных человека, генерации биометрического кода из биометрических данных или комбинации фрагментов биометрических данных человека, сбора уникальных идентификационных данных IoT устройства, генерации кода IoT устройства из уникальных идентификационных данных IoT устройства, вставки в поле расширения сертификата открытого ключа, хранящегося в портативном устройстве, проверочного кода, содержащего биометрический код и код IoT устройства, генерации пары, содержащей закрытый ключ и открытый ключ, причем закрытый ключ содержит проверочный код и передачу открытого ключа на удаленный объект, связанный с IoT устройством, с обеспечением тем самым возможности регистрации человека удаленным объектом в качестве авторизованного пользователя IoT устройства. 4 н. и 24 з.п. ф-лы,



RU 2702076 C2

RU 2702076 C2

25 ил.




Фиг. 1A

RU 2702076 C2

RU 2702076 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 702 076**(13) **C2**

(51) Int. Cl.
*H04L 9/32* (2006.01)
*G06F 21/33* (2013.01)
*G06F 21/32* (2013.01)
*H04W 12/06* (2009.01)

## (12) ABSTRACT OF INVENTION

(52) CPC
*H04L 9/3231 (2013.01); H04L 63/0823 (2013.01); G06F 21/31 (2013.01); H04W 12/06 (2013.01)*

(21)(22) Application: **2017140260, 23.04.2015**

(24) Effective date for property rights:
**23.04.2015**

Registration date:
**03.10.2019**

Priority:
(22) Date of filing: **23.04.2015**

(43) Application published: **23.05.2019** Bull. № **15**

(45) Date of publication: **03.10.2019** Bull. № **28**

(85) Commencement of national phase: **23.11.2017**

(86) PCT application:
**KR 2015/004048 (23.04.2015)**

(87) PCT publication:
**WO 2016/171295 (27.10.2016)**

Mail address:
**191002, Sankt-Peterburg, a/ya 5, Obshchestvo s ogranichennoj otvetstvennostyu "Lyapunov i partnery"**

(72) Inventor(s):
**CHOI Unho (KR)**

(73) Proprietor(s):
**CHOI Unho (KR)**

RU 2702076 C2

## (54) AUTHENTICATION IN DISTRIBUTED ENVIRONMENT

(57) Abstract:

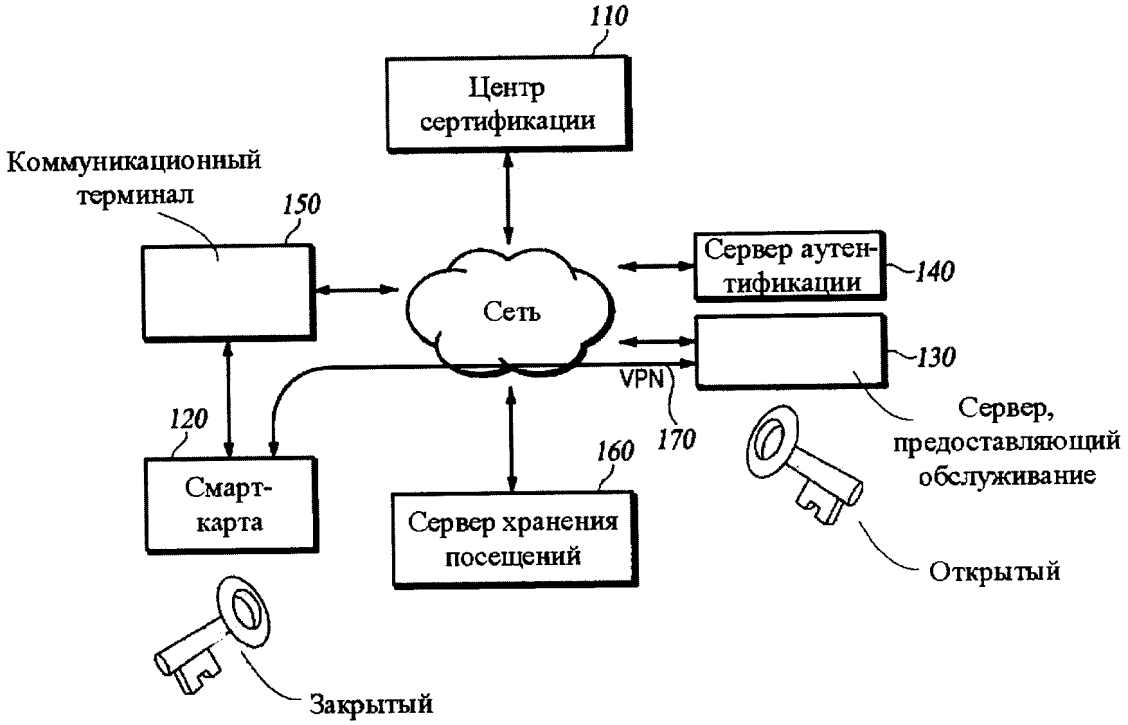
FIELD: physics.

SUBSTANCE: invention relates to computer engineering. Technical result is achieved by collecting by means of a portable device biometric data or a combination of fragments of biometric data of a person, generating a biometric code from biometric data or a combination of fragments of biometric data of a person, collecting unique identification data of the IoT device, generating an IoT device code from the IoT device unique identification data, inserting a public key certificate stored in the portable device in the extension field, a verification code containing a biometric code and an IoT device code, generating a pair comprising a private key and an open key, the private key comprising a verification code and transmitting the public key to a remote object associated with the IoT device, thereby enabling the person to register the remote object as an authorized user of the IoT device.

EFFECT: technical result consists in improvement of information security of remote connection of computer system.

28 cl, 25 dwg

RU 2702076 C2




Фиг. 1A

RU 2702076 C2

RU 2702076 C2

Область техники, к которой относится изобретение

[0001] Настоящее изобретение относится к аутентификации пользователя и аутентификации IoT (Интернет вещей) устройства в распределенной среде, в том числе онлайн и офлайн аутентификациям.

Уровень техники

[0002] Утверждения в этом разделе просто предоставляют справочную информацию, связанную с настоящим изобретением, и могут не обязательно представлять предшествующий уровень техники.

[0003] Применения Интернета вещей (IoT) обсуждаются во всех отраслях. Например, IoT пытаются применить для удаленного управления и контролирования объекта, к которому трудно получить доступ, такому как плотина, атомная электростанция, и тому подобному, и системы управления движением, а также персонального устройства, такого как смарт-телевизор, робот-пылесос, автомобильный навигатор, и тому подобное, и различных удаленных услуг, предоставляемых при облачном обслуживании. Однако, IoT устройство и IoT система, имеющие функцию коммуникации и функцию автономного получения и обработки данных, подвержены кибератакам из-за нечеткой взаимосвязи между используемым предметом и его владельцем.

[0004] В частности, устройства IoT, составляющие в настоящее время сеть IoT, обычно имеют простую вычислительную функцию и уязвимую защиту и, следовательно, уязвимы для атаки извне. Из-за особенностей IoT сети уязвимость защиты в конкретной зоне и кибератака, направленная на эту уязвимость, может вызвать неблагоприятные последствия, которые могут повлиять на другие производственные зоны.

[0005] Поскольку в IoT устройстве, имеющем простую функцию коммуникации, невозможно по отдельности установить и приводить в действие защитное программное обеспечение, требуются дополнительные усилия для того, чтобы встроить аппаратный модуль защиты в IoT устройство или тому подобное, чтобы применить защитное решение для всей системы. Примеры проблемы защиты в IoT включают в себя ситуацию, когда вредоносный код заражает IoT устройство или сеть, так что важная информация утекает или искажается, что вызывает системный сбой, и злоумышленник свободно управляет IoT устройством или сетью дистанционно. В частности, доступ в сеть с терминала, зараженного вредоносным кодом, может нанести сети серьезный ущерб. Например, может случиться, что автоматизированное транспортное средство, электромобиль или интеллектуальное транспортное средство дистанционно управляются так, чтобы вызвать аварию, а медицинское устройство в больнице не функционирует, угрожая жизни пациента.

[0006] В IoT сети должна быть обеспечена целостность IoT устройства, и должно быть четко известно, надежное или нет IoT устройство присоединяется к сети, и должно быть удостоверено, осуществляется доступ в сеть легальным пользователем или нет.

[0007] В системе с обычной информационной защитой незаконный пользователь может получить личную информацию, пароль и биометрические данные легального пользователя, которые используются для проникновения в сеть. В качестве другого примера, поскольку информация о персональной аутентификации практически не содержатся в сертификате открытого ключа, выданном центром сертификации, существует уязвимость, из-за которой третья сторона может похитить сертификат открытого ключа и пароль сертификата для незаконного их использования. Кроме того, если человек удаленно обращается к бизнес-системе компании или государственного учреждения, используя легальный терминал, с помощью похищенной информации аутентификации, такой как ID, пароль или биометрические данные

легального пользователя, он или она может свободно использовать бизнес-систему без какого-либо препятствия. Типичным примером проблемы с безопасностью является то, что, если у кого-либо есть электронная ID-карта, содержащая микросхему сотрудника компании, подобранная на улице, например, он или она может присвоить фотографию или тому подобное и использовать ее у входа в компанию, как будто он или она является авторизованным пользователем. Кроме того, в прессе сообщалось о случае взлома, где ID, пароль, биометрические данные, токен, OTP (одноразовый пароль) и PKI (инфраструктура открытых ключей) сертификат используются по отдельности без их объединения для многофакторной аутентификации, а злоумышленник изменяет и нарушает их в середине, чтобы взломать сеть.

Настоящее изобретение в некоторых вариантах осуществления предлагает способ для аутентификации пользователя и аутентификации IoT устройства в распределенной среде, в том числе онлайн и офлайн аутентификации, а также предлагает инструмент, использующий этот способ, и систему аутентификации.

Раскрытие сущности изобретения

[0008] Согласно некоторым вариантам осуществления настоящего изобретения, зашифрованные биометрические данные, которые зашифрованы на основе сертификата открытого ключа, заранее хранятся в устройстве пользователя (например, смарт-карте, коммуникационном терминале или тому подобном), и аутентификация пользователя (первая аутентификация пользователя) производится посредством биометрического сопоставления в устройстве. Далее сертификат открытого ключа, соответствующий зашифрованным биометрическим данным, используется для выполнения аутентификации пользователя (вторая аутентификация пользователя) для авторизации транзакции на сервере, предоставляющем обслуживание. Более того, в соответствии с некоторыми вариантами осуществления настоящего изобретения используются одноразовый пароль, нажатие клавиш, динамическая подпись, информация о местоположении и тому подобное в качестве дополнительных факторов аутентификации для усиления безопасности первой и второй аутентификаций пользователя. Кроме того, в соответствии с некоторыми вариантами осуществлениями настоящего изобретения, механизм аутентификации, включающий в себя первую и вторую аутентификации пользователя, применяется для контроля доступа к IoT устройству.

[0009] В соответствии с некоторыми вариантами осуществления настоящего изобретения, способ регистрации пользователя в системе управления аутентификацией на основе сертификата открытого ключа, который выполняется с портативным устройством пользователя, включает в себя: шифрование биометрических данных или комбинации фрагментов биометрических данных пользователя с помощью алгоритма шифрования, определенного в сертификате открытого ключа, хранение зашифрованных биометрических данных или зашифрованной комбинации фрагментов биометрических данных в портативном устройстве, маркирование зашифрованных биометрических данных или зашифрованной комбинации фрагментов биометрических данных для генерации биометрического кода, генерацию пары ключей, включающей в себя закрытый ключ и открытый ключ, путем вставки проверочного кода, содержащего по меньшей мере биометрический код в поле расширения сертификата открытого ключа, передачу открытого ключа удаленному объекту и запрос регистрации пользователя.

[0010] В некоторых вариантах осуществления поле расширения сертификата открытого ключа включает в себя, помимо биометрического кода по меньшей мере одно из: первого добавочного кода, формируемого из уникальной идентификационной информации или отличительных данных, закрепленных за портативным устройством,

второго добавочного кода, формируемого из информации о местоположении, указывающей положение, где запрашивается аутентификация пользователя, третьего добавочного кода, формируемого из уникальных личных данных, закрепленных за пользователем, четвертого добавочного кода, формируемого из характеристической информации, указывающей на характеристики поведения пользователя, или пятого добавочного кода, формируемого из отличительных данных прибора, закрепленных за IoT устройством.

[0011] В соответствии с некоторыми вариантами осуществления настоящего изобретения, способ аутентификации пользователя в системе управления аутентификацией, основанный на сертификате открытого ключа, который выполняется с помощью портативного устройства пользователя, хранящего закрытый ключ, в который вставлен проверочный код, включающий в себя биометрический код, и зашифрованные биометрические данные или зашифрованную комбинацию фрагментов биометрических данных, из которых сформирован биометрические код, включает в себя сбор биометрических данных или комбинации фрагментов биометрических данных пользователя, сравнение биометрических данных или комбинации фрагментов биометрических данных пользователя по меньшей мере с одним набором зашифрованных биометрических данных или зашифрованной комбинацией фрагментов биометрических данных, хранящихся в портативном устройстве, или с биометрическим кодом, передачу на удаленный объект информации об аутентификации, включающей в себя проверочный код, вставленный в закрытый ключ, когда биометрические данные или комбинация фрагментов биометрических данных пользователя соответствует по меньшей мере одному из: зашифрованных биометрических данных или зашифрованной комбинации фрагментов биометрических данных, и запрос об аутентификации пользователя.

[0012] В соответствии с некоторыми вариантами осуществления настоящего изобретения, способ управления аутентификацией пользователя в системе управления аутентификацией на основе сертификата открытого ключа, который выполняется с помощью удаленного объекта, связанного с портативным устройством пользователя через сеть, включает в себя прием от портативного устройства открытого ключа, соответствующего закрытому ключу, в который вставлен проверочный код, включающий в себя биометрический код, сформированный из биометрических данных или из комбинации фрагментов биометрических данных пользователя, выполнение регистрации пользователя на основе открытого ключа, получение от портативного устройства информации об аутентификации, включающей в себя проверочный код, вставленный в закрытый ключ, проверку информации об аутентификации на основе открытого ключа и выполнение аутентификации пользователя на основе результата проверки.

[0013] В соответствии с некоторыми вариантами осуществления настоящего изобретения, способ управления аутентификацией пользователя в системе управления аутентификацией на основе сертификата открытого ключа, который выполняется открытым терминалом, выполненным с возможностью предоставления заданного обслуживания, и сервером, предоставляющим обслуживание, выполненным с возможностью управлять открытым терминалом, включает в себя: получение, в том числе, сервером, обеспечивающим обслуживание, от портативного устройства пользователя открытого ключа, соответствующего закрытому ключу, в который вставлен проверочный код, включающий в себя биометрический код, сформированный из биометрических данных или комбинации фрагментов биометрических данных

пользователя, выполнение в том числе сервером, предоставляющим сервис, регистрации пользователя на основе открытого ключа, получение, в том числе, открытым терминалом, от портативного устройства информации аутентификации, включающей в себя проверочный код, вставленный в закрытый ключ, запрос, в том числе, с открытого терминала, сервера, предоставляющего обслуживание, на выполнение проверки информации об аутентификации на основе открытого ключа, выполнение, в том числе, открытым терминалом, аутентификации пользователя на основе результатов проверки, и предоставление, в том числе, открытым терминалом, предусмотренного обслуживания, когда аутентификация пользователя прошла успешно.

[0014] В соответствии с некоторыми вариантами осуществления настоящего изобретения, предлагается усиленная функция аутентификации обслуживания. Биометрические данные кодируются или маркируются и вставляются в поле расширения сертификата открытого ключа с помощью сертификата открытого ключа, тем самым предотвращая фальсификацию зашифрованных биометрических данных или электронной подписи, хранящейся в смарт-карте (или коммуникационном терминале), путем использования сертификата открытого ключа (то есть биометрического сертификата). Кроме того, различные варианты осуществления настоящего изобретения могут быть применены к системе учета, электронной платежной системе, электронной карточке резидента, выдаче паспорта или пенсии, страхованию, транспортной карте, электронным выборам, электронному кошельку и купону, выпущенному государством, государственному учреждению, финансовому учреждению и тому подобному. В этом случае, даже если третья сторона имеет простую персональную информацию: информацию о карте, биометрические данные или информацию о сертификате конкретного пользователя, незаконное использование этих фрагментов информации третьей стороной может быть предотвращено.

[0015] В соответствии с некоторыми вариантами осуществления настоящего изобретения, информационная безопасность для удаленного подключения рабочей системы может быть усилена.

Краткое описание чертежей

[0016] Вышеупомянутые и другие задачи, признаки и преимущества настоящего изобретения очевидны из последующего подробного описания со ссылками на прилагаемые чертежи, на которых:

[0016] На фиг. 1A приведена схема системы управления аутентификацией пользователя в распределенной среде в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0017] На фиг. 1B приведена схема системы управления удостоверением личности в распределенной среде, в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0018] На фиг. 2A-2C приведены схемы представления способов связи между коммуникационным терминалом и смарт-картой, в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0019] На фиг. 3A приведена схема для представления иерархической структуры смарт-карты, в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0020] На фиг. 3B приведена схема представления физической структуры смарт-карты, в соответствии с некоторыми вариантами настоящего изобретения.

[0021] На фиг. 3C приведена схема представления функциональной структуры смарт-карты, в соответствии с некоторыми вариантами осуществления настоящего

изобретения.

[0022] На фиг. 4A приведена функциональная схема процедуры регистрации пользователя в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0023] На фиг. 4B приведена функциональная схема процедуры регистрации пользователя в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0024] На фиг. 5A и 5B приведены схемы форматов сертификатов открытого ключа, применяемых в системе управления аутентификацией пользователя в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0025] На фиг. 6 приведена схема примерного формата кода, хранящегося в домене EV (расширенной проверки) открытого ключа/закрытого ключа, показанного на фиг. 5B и примерный формат информации аутентификации, передаваемой со смарт-карты.

[0026] На фиг. 7A приведена функциональная схема процедуры аутентификации пользователя в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0027] На фиг. 7B приведена функциональная схема процедуры аутентификации пользователя в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0028] На фиг. 8A и 8B приведены схемы конфигурации системы для управления пользователем IoT устройством в распределенной среде в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0029] На фиг. 9A приведена функциональная схема процедуры регистрации пользователя устройства в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0030] На фиг. 9B приведена функциональная схема процедуры регистрации пользователя устройства в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0031] На фиг. 10A приведена функциональная схема процедуры аутентификации пользователя устройства в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0032] На фиг. 10B приведена функциональная схема процедуры аутентификации пользователя устройства в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0033] На фиг. 11 приведена схема, иллюстрирующая концепцию распределенной системы аутентификации применительно к онлайн/офлайн среде.

[0034] На фиг. 12 приведена функциональная схема процедуры аутентификации пользователя в офлайн среде, в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0035] На фиг. 13 приведена таблица примерной области применения, в которой могут быть применены варианты осуществления настоящего изобретения.

[0036] На фиг. 14 приведена схема для иллюстрации случая, когда различные фрагменты биометрических данных или их комбинация могут быть распределены и использованы в различных применениях.

Осуществление изобретения

[0037] Далее здесь будет подробно описан по меньшей мере один вариант осуществления настоящего изобретения со ссылкой на прилагаемые чертежи. В последующем описании сходные ссылочные позиции обозначают сходные элементы,

хотя элементы показаны на разных чертежах. Кроме того, в последующем описании по меньшей мере одного варианта осуществления изобретения подробное описание известных функций и конфигураций, объединенных в настоящем документе, будет опущено с целью обеспечения ясности и краткости.

[0038] Кроме того, при описании компонентов настоящего изобретения используются такие термины, как первый, второй, A, B, (a) и (b). Они предназначены исключительно для того, чтобы отличить один компонент от другого, и специалисту в области техники очевидно, что термины не подразумевают и не предлагают содержание, порядок или последовательность компонентов.

[0039] Везде в данном описании, когда часть "включает в себя" или "содержит" компонент, если только не существует конкретного описания, противоречащего этому, часть может дополнительно включать в себя другие компоненты, не исключая другие компоненты. Кроме того, такие термины в данной детализации как "блок", "модуль" и другие, означает блоки для выполнения по меньшей мере одной функции или операции, которая может быть реализована аппаратно, программно или комбинацией того и другого. Кроме того, "Интернет-вещей (IoT)" во всеобъемлющем значении этого термина, используемого в описании настоящего изобретения, включает в себя M2M (машина-машина), MTC (коммуникации машинного типа), SDC (коммуникация через интеллектуальное устройство) и MOC (машинно-ориентированные коммуникации), как они именуются различными органами по стандартизации.

[0040] На фиг. 1A приведена схема системы управления аутентификацией пользователей в распределенной среде, в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0041] Система управления аутентификацией пользователей, как показано на фиг. 1A, включает в себя центр 110 сертификации (CA), смарт-карту 120, сервер 130, предоставляющий обслуживание, сервер 140 аутентификации, коммуникационный терминал 150 и сервер 160 хранения загрузок.

[0042] Центр 110 сертификации выдает сертификат открытого ключа, содержащий информацию о центре сертификации (версия, дата истечения срока действия, алгоритм, выдающее учреждение и тому подобное). В процессе регистрации пользователя сертификат открытого ключа преобразуется в сертификат открытого ключа, соответствующий биометрическим данным пользователя. То есть сертификат открытого ключа используется для создания открытого ключа/закрытого ключа, в который вставлен код, соответствующий биометрическим данным пользователя. В некоторых вариантах осуществления сертификат открытого ключа является сертификатом на основе инфраструктуры открытого ключа (PKI) или закрытым сертификатом. Сертификат открытого ключа выдается пользователю, как правило, с сервера центра 110 сертификации (CA); однако, в некоторых случаях он предварительно устанавливается в безопасной зоне (например, микросхеме, защищенном элементе (SE), доверенной исполняемой среде (TEE), операционной системе, процессоре, памяти, облачном SE, и тому подобном) коммуникационного терминала или смарт-карты при проектировании или изготовлении продукта.

[0043] Смарт-карта 120 хранит закрытый ключ, зашифрованные биометрические данные для сравнения с распознаваемыми биометрическими данными и другие фрагменты информации во встроенном биометрическом датчике, микросхеме, памяти или чем-либо подобном. Кроме того, в закрытый ключ вставляется биометрический код, создаваемый путем кодирования (или маркирования) зашифрованных биометрических данных.

[0044] Смарт-карта 120 зашифровывает биометрические данные пользователя на основе сертификата открытого ключа, и кодирует (или маркирует) зашифрованные биометрические данные для генерации биометрического кода. Смарт-карта 120 генерирует пару ключей (то есть открытый ключ и закрытый ключ) путем вставки сгенерированного биометрического кода в сертификат открытого ключа. Биометрический код или закрытый ключ используется для проверки целостности и отсутствия нарушения зашифрованных биометрических данных, которые могут быть использованы в качестве биологической подписи. Биометрический код, сгенерированный указанным выше методом, может быть использован в качестве маркера или может использоваться в комбинации с OTP (одноразовым паролем; также называемым "динамическим кодом"). Биометрические данные, закодированные и вставленные в публичный ключ, содержат информацию об отпечатке пальца, информацию о кровеносных сосудах, голосовую информацию, информацию о радужной оболочке, информацию о почерке, физиономическую информацию, о сердцебиении и тому подобное. Смарт-карта 120 передает открытый ключ серверу 130, предоставляющему обслуживание, или серверу 140 аутентификации, а сервер, предоставляющий обслуживание, и сервер аутентификации позднее использует полученный открытый ключ в процессе аутентификации.

[0045] В некоторых вариантах осуществления изобретения смарт-карта 120 объединяет биометрические коды, соответственно закодированные, из множества фрагментов различных биометрических данных пользователя и вставляет объединенные биометрические коды в единый сертификат. Например, может быть использована комбинация различных типов биометрических данных, таких как отпечаток пальца + радужная оболочка, лицо + голос, сердцебиение + радужная оболочка, и комбинация подобных типов биометрических данных, таких как отпечаток пальца 1 (большой палец) + отпечаток пальца 2 (указательный палец) и радужная оболочка 1 (правая) + радужная оболочка 2 (левая). При использовании комбинации множества фрагментов биометрических данных в качестве дополнительного элемента аутентификации может быть добавлен порядок ввода биометрических данных (например, отпечаток пальца 1 → отпечаток пальца 2 → отпечаток пальца 3 → радужная оболочка). В некоторых вариантах осуществления смарт-карта вставляет различные фрагменты биометрических данных или различные комбинации фрагментов биометрических данных пользователя в различные сертификаты открытого ключа. В некоторых вариантах осуществления коды, извлекаемые из физической подписи (собственноручной подписи или динамической подписи) или нажатия клавиши пользователем, способа ввода биометрических данных и тому подобного, добавляются в сертификат в качестве добавочного элемента аутентификации. В этом случае время, скорость, направление, давление, информацию о местоположении и тому подобную информацию, которая является характеристиками поведения (или элементами шаблона поведения) при введении пользователем физической подписи или нажатии клавиш для ввода слова или числа, имеющего определенное значение, можно рассматривать как добавочный элемент аутентификации.

[0046] Далее, в некоторых вариантах осуществления смарт-карта 120 выполняется с возможностью генерировать пару ключей путем соединения одного или большего количества добавочных кодов с биометрическим кодом, как добавочным элементом назначения или аутентификации,. Например, по меньшей мере один из: добавочного кода, полученного из уникальных идентификационных данных, закрепленных в смарт-карте 120, добавочного кода, сформированного из информации о местоположении, указывающей на позицию, из которой запрашивается аутентификация (или регистрации)

пользователя, добавочного кода, сформированного из уникальных идентификационных данных, закрепленных за пользователем, добавочного кода, сформированного из характеристической информации, указывающей характеристики поведения пользователя, или добавочного кода, сформированного из данных идентификации устройства, закрепленный за IoT устройством, может быть соединен с биометрическим кодом.

[0047] Кроме того, смарт-карта 120 сконфигурирована так, чтобы при генерации пары ключей (открытый ключ/закрытый ключ) путем вставки биометрического кода в сертификат открытого ключа генерировать множество биометрических кодов из различных фрагментов биометрических данных или комбинации фрагментов биометрических данных, а также вставлять множество биометрических кодов в поле расширения сертификата открытого ключа определенным образом. Вышеуказанный один или большее количество дополнительных кодов может быть соединен с каждым из биометрических кодов. Следовательно, закрытый ключ и открытый ключ включают в себя множество биометрических кодов или множество биометрических кодов с присоединенными добавочными кодами. В этом случае множество биометрических кодов может использоваться для отличающихся друг от друга целей. Например, любой из множества биометрических кодов предназначен для использования при выполнении обычной аутентификации пользователя закрытым ключом. Остальные биометрические коды могут быть предназначены для извещения о принудительном использовании закрытого ключа третьей стороной, для запроса отмены регистрации пользователя, выполненной на основе переданного открытого ключа, для запроса инициализации системы управления аутентификацией, которая управляется удаленным объектом (например, сервером, предоставляющим обслуживание, сервером аутентификации, централизованным контроллером или тому подобным), и тому подобного.

[0048] Коммуникационный терминал 150, связанный со смарт-картой 120 проводным или беспроводным образом, устанавливает виртуальную частную сеть (VPN) между смарт-картой 120 и сервером 130, предоставляющим обслуживание, в ответ на сигнал запуска туннелирования, полученный от смарт-карты 120, получает информацию об аутентификации на основе зарегистрированного сертификата от смарт-карты 120, и передает информацию об аутентификации в сервер 130, предоставляющий обслуживание. Кроме того, коммуникационный терминал 150 может быть использован в качестве средства для сбора биометрических данных и динамической подписи пользователя, данных идентификации IoT устройства, и подтверждения, требуемого при процедуре регистрации пользователем или процедуре аутентификации пользователя, для генерации закрытого ключа и открытого ключа смарт-карты 120. В некоторых вариантах осуществления коммуникационный терминал 150 включает в себя один или большее количество биометрических датчиков, сенсорный экран, видеокамеру, микрофон и тому подобное, или подключен к ним. Коммуникационный терминал 150 включает в себя терминал открытого обслуживания (ATM (банкомат), Kiosk (банковский пункт интернет-связи), POS (точку продаж), и тому подобное), а также отдельный терминал связи (например, мобильный телефон, планшетный ПК, настольный компьютер, ноутбук, и тому подобное), и подразумевает охват всех устройств, которые могут связываться с удаленным объектом в коммуникационной сети.

[0049] Сервер аутентификации проверяет информацию об аутентификации, передаваемую от смарт-карты (или коммуникационного терминала) с помощью открытого ключа, полученного при процедуре регистрации пользователя. Например, сервер аутентификации получает открытый ключ, сгенерированный смарт-картой (или коммуникационным терминалом) с помощью сертификата открытого ключа при

процедуре регистрации пользователя, а затем при процедуре аутентификации пользователя проверяет информацию об аутентификации, передаваемую от смарт-карты (или коммуникационного терминала) на основе открытого ключа в ответ на запрос от сервера, предоставляющего обслуживание.

[0050] Сервер 130, предоставляющей обслуживание, является сервером поставщика услуг, который предоставляет пользователю, проходящему аутентификацию, различные сервисы, включая обслуживание банковских/кредитных карт, платежный сервис, сервис электронного государства, облачный сервис, сервис, связанный с IoT устройствами, аварийную службу, и тому подобное. Сервер 130, предоставляющий обслуживание, проверяет подлинность пользователя на основе информации об аутентификации, полученной от смарт-карты (или коммуникационного терминала). Например, сервер, предоставляющий обслуживание, отправляет запрос серверу аутентификации о проверке информации об аутентификации и проверяет подлинность пользователя на основе результата проверки. В некоторых вариантах осуществления сервер, предоставляющий обслуживание, и сервер аутентификации реализуются как функциональные составные элементы на одном сервере.

[0051] Сервер 160 хранилища загрузок записывает данные регистрации, показывающие историю подключений смарт-карты 120 к серверу, предоставляющему обслуживание, через коммуникационный терминал 150, и результат аутентификации. Кроме того, когда сервер 130, предоставляющий обслуживание, обращается к центру сертификации, серверу компании, обслуживающей карты, или тому подобному, чтобы подтвердить информацию о пользователе, сервер 160 хранилища загрузок записывает и хранит попытку доступа к нему и результат попытки доступа. Кроме того, сервер 160 хранения загрузок отслеживает сеть VPN 170, установленную между смарт-картой 120 и сервером 130, предоставляющим обслуживание, и выполняет функцию межсетевого экрана сети VPN, чтобы запретить доступ нелегальному пользователю. Кроме того, сервер хранения загрузок подтверждает, является пользователь легальным пользователем электронного кошелька или нет, и выдает или печатает электронную квитанцию, включающую в себя биометрический код данного пользователя.

[0052] Данные, хранящиеся на сервере 160 хранения загрузок, могут использоваться в цифровой криминалистике. Например, данные журнала могут быть использованы позже в качестве подтверждения/доказательства поведения пользователя. Например, информация об аутентификации, передаваемая от смарт-карт к серверу 130, предоставляющему обслуживание, содержит информацию о рукописной подписи пользователя, и при сохранении такой информации о рукописной подписи пользователя в данных журнала, информация о физической подписи может быть позже отображена в печатном виде или в электронном виде на электронной квитанции или счете.

[0053] На фиг. 1B приведена схема системы управления идентификацией в распределенной среде, в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0054] Смарт-карта 120 и коммуникационный терминал 150 представлены раздельно на фиг 1A; однако, как показано на фиг. 1B, в соответствии с некоторыми вариантами осуществления настоящего изобретения, функция смарт-карты 120 встроена в коммуникационный терминал 150. То есть сертификат, соответствующий биометрическим данным пользователя, может храниться и управляться в защищенном элементе (SE; защищенных памяти и среде выполнения), центральном процессоре CPU, операционной системе OS или тому подобном в коммуникационном терминале 150. Элемент защиты в коммуникационном терминале 150 может быть реализован, например,

в микросхеме, такой как SIM, USIM, карта MicroSD, NFC-карта и тому подобном.

[0055] Коммуникационный терминал 150 способен выполнять процедуру аутентификации пользователя, используя сертификат, соответствующий биометрическим данным пользователя, без соединения со смарт-картой. Кроме того, коммуникационный терминал включает в себя различные типы биометрических датчиков для измерения биометрических данных, и включает в себя соответствующее входное/зондирующее средство для получения информации об устройстве от IoT устройства или связан с внешним устройством, включающим в себя такое средство. Коммуникационный терминал 150, хотя и не отмечен специально, имеет признаки, соответствующие различным признакам, присущим функциям или операциям со смарт-картой, описанным в общих вариантах осуществления настоящего изобретения.

[0056] В некоторых вариантах осуществления коммуникационный терминал, показанный на фиг. 1B, включает в себя персональный коммуникационный терминал (например, мобильный телефон, носимое устройство, такое как часы, очки, кольцо или тому подобное, планшетный ПК, настольный компьютер, ноутбук и тому подобное), и подразумевает охват всех устройств, которые могут связываться с удаленным объектом в коммуникационной сети.

[0057] На фиг. 2A-2C приведены схемы для способов установления связи между коммуникационным терминалом и смарт-картой в соответствии с некоторыми вариантами осуществления настоящего изобретения. На фиг. 2A-2C предполагается, что коммуникационный терминал, показанный на фиг. 1, реализован посредством мобильного терминала, такого как смартфон.

[0058] В некоторых вариантах осуществления изобретения, как показано на фиг. 2A, смарт-карта сконфигурирована для связи с коммуникационным терминалом через карманный шифратор. Этот шифратор выполнен с возможностью передавать или принимать информацию на смарт-карту или с нее контактным или бесконтактным образом. Шифратор подключается, например, в аудио разъем и микро USB порт смартфона. При такой конфигурации пользователь может связать смартфон и коммуникационной терминал, подключив шифратор к смартфону и прикладывая или проводя смарт-картой у шифратора. В некоторых вариантах осуществления шифратор обеспечивает аппаратную схему шифрования в целях безопасности.

[0059] В соответствии с некоторыми вариантами осуществления, как показано на фиг. 2B, смарт-карта непосредственно подключается к коммуникационному терминалу, устанавливая связь через схему беспроводной связи (например, NFC (ближняя бесконтактная связь), RFID (радиочастотная идентификация) или подобную).

[0060] В соответствии с некоторыми вариантами осуществления, как показано на фиг. 2C, смарт-карта реализована как тип USB шифратора, который напрямую подключается к коммуникационному терминалу.

[0061] На фиг. 3A приведено схематическое представление иерархической структуры смарт-карты в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0062] Физическая иерархия смарт-карты включает в себя процессор, память и порт ввода-вывода. Память включает в себя одну любую из: постоянной памяти (ROM), памяти с произвольным доступом (RAM), электрически стираемую программируемую постоянную память (EEPROM), стираемую программируемую ROM (EPROM), флэш-память EEPROM, ферроэлектрическую RAM (FeRAM), и их комбинации. Избирательно смарт-карта дополнительно включает в себя по меньшей мере одно из: дисплея или одного или большего количества биометрических датчиков. Избирательно смарт-карта

дополнительно включает в себя схему физически неклонируемой функции (PUF).

[0063] Иерархия приложений смарт-карты относится к функциональному составному элементу операционной системы или апплету на смарт-карте, который распределяется, например, на модуль сбора биометрической информации, управляющий модуль биометрической информации, модуль биометрической аутентификации, модуль сбора информации об устройстве, модуль управления VPN-сети, модуль генерации OTP (одноразового пароля) модуль управления ключами и модуль исполнения аутентификации. Каждый функциональный составной элемент описан далее со ссылкой на фиг. 3C.

[0064] На фиг. 3B приведена схема для представления физической структуры смарт-карты в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0065] Как показано на фиг. 3B, в некоторых вариантах осуществления смарт-карта 300 включает в себя микросхему 301, содержащую процессор/память/OS/PUF, электрические цепи и тому подобное, по меньшей мере один биометрический датчик 303 и дисплей 304.

[0066] Смарт-карта 300, показанная на фиг. 3B, выполнена с возможностью воспринимать по меньшей мере часть одного или большего количества фрагментов биометрических данных, требуемых для процедуры регистрации пользователя и процедуры аутентификации пользователя, с помощью встроенного биометрического датчика 303. Биометрический датчик 303 включает в себя датчик распознавания отпечатков пальцев, датчик распознавания радужной оболочки, датчик распознавания голоса, датчик распознавания кровеносных сосудов, датчик распознавания рукописного ввода, лицевой датчик, датчик сердцебиения, датчик динамической подписи и тому подобного. В частности, датчик динамической подписи выполнен с возможностью соединения с дисплеем 304, содержащим сенсорный экран.

[0067] Смарт-карта 300 выполнена с возможностью отображения одноразового пароля (OTP), генерируемого модулем генерации OTP, входящим в состав операционной системы/процессора/памяти и тому подобного, на микросхеме 301. Смарт-карта 300 выполнена с возможностью дополнительно отображать следующую информацию на дисплее 304:

- результат биометрического сопоставления;
- уведомление о том, что закрытого ключа, соответствующего входным биометрическим данным или комбинации фрагментов биометрических данных, не существует;
- перечень множества закрытых ключей, соответствующих входным биометрическим данным, или комбинации фрагментов биометрических данных;
- использование закрытого ключа, соответствующего входным биометрическим данным или комбинации фрагментов биометрических данных; и
- зарегистрированную динамическую подпись.

[0068] На фиг. 3C приведено схематическое представление функциональной структуры смарт-карты в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0069] Каждый составной элемент смарт-карты, показанный на фиг. 3C, является функциональным элементом, логически разделенным или функциональным составным элементом, соединенным с физическим составным элементом. То есть каждый составной элемент соответствует функциональному составному элементу, служащему для достижения технического замысла настоящего изобретения, и поэтому, даже если каждый составной элемент выполняет свою функцию в комплексе или отдельно, его

следует интерпретировать как входящий в пределы правовой охраны настоящего изобретения до тех пор, пока функция, выполняемая функциональной конфигурацией настоящего изобретения, не будет достигнута. Кроме того, разумеется, если составной элемент выполняет одну и ту же или аналогичную функцию, его следует интерпретировать как входящий в пределы правовой охраны настоящего изобретения независимо от названия.

[0070] Как показано на фиг. 3C, функциональные элементы смарт-карты можно разделить на модуль 311 сбора биометрической информации, модуль 312 управления биометрической информацией, модуль 313 управления ключами, модуль 314 биометрической аутентификации, модуль 315 управления VPN, модуль 316 исполнения аутентификации, модуль 317 генерации OTP и модуль 318 сбора информации об устройстве.

[0071] Модуль 311 сбора биометрической информации собирает биометрические данные пользователя при процедуре регистрации пользователя и при процедуре аутентификации пользователя. В некоторых вариантах осуществления модуль 311 сбора биометрической информации получает биометрические данные пользователя от биометрического датчика, встроенного в смарт-карту 310. В некоторых вариантах осуществления изобретения, модуль 311 сбора биометрической информации получает биометрические данные зондирования от коммуникационного терминала или других внешних устройств (например, ATM, Kiosk, POS, считывателя карт тому подобного), в том числе биометрического датчика.

[0072] Модуль 312 управления биометрической информацией зашифровывает биометрические данные, собранные модулем 311 сбора биометрической информации при процедуре регистрации пользователя, на основе сертификата открытого ключа, и сохраняет и компонует зашифрованные биометрические данные в смарт-карте (например, в памяти, встроенной в микросхему смарт-карты, в биометрическом датчике, встроенном в смарт-карту, и тому подобном). В некоторых вариантах осуществления модуль 312 управления биометрической информацией зашифровывает и хранит множество фрагментов биометрических данных абонента. Например, информация об отпечатках пальцев для каждого пальца абонента хранится в смарт-карте, и информация о радужной оболочке глаз абонента хранится в смарт-карте. Кроме того, в смарт-карте хранятся различные комбинации фрагментов биометрических данных абонента, такие как отпечаток пальца + радужная оболочка, радужная оболочка + лицо и тому подобное.

[0073] Модуль 313 управления ключами генерирует биометрический код путем кодирования (или маркирования) зашифрованных биометрических данных на основе сертификата открытого ключа и генерирует пару ключей (закрытый ключ и открытый ключ), в которые вставлен биометрический код путем внесения сгенерированного биометрического кода в сертификат 110 открытого ключа. Модуль 313 управления ключами устанавливает или хранит сгенерированный закрытый ключ в памяти, CPU, OS, приложении или тому подобном, встроенном в микросхему смарт-карты, и передает сгенерированный открытый ключ серверу аутентификации (или серверу, предоставляющему обслуживание). В некоторых вариантах осуществления изобретения модуль 313 управления ключами выполнен с возможностью создания пары ключей путем объединения с биометрическим кодом одного или большего количества добавочных кодов в качестве добавочного элемента назначения или аутентификации. Во избежание путаницы, сертификат открытого ключа, используемый для генерации пары ключей, то есть сертификат открытого ключа, в который не вставлен биометрический код, далее называется "пустым сертификатом".

[0074] В некоторых вариантах осуществления изобретения пустой сертификат устанавливается или хранится на смарт-карте заранее. То есть государство/производитель/финансовый агент/поставщик услуг устанавливает или хранит по меньшей мере один пустой сертификат в микросхеме, OS, CPU, памяти или в чем-то подобном на смарт-карте заранее, на этапе изготовления/выпуска смарт-карты. В этом случае предпочтительно разрешить хранить сертификат в смарт-карте только учреждению, выпускающему смарт-карту 120. В некоторых вариантах осуществления смарт-карта выпускается с пустым сертификатом с сервера центра сертификации (CA) через коммуникационный терминал. В некоторых вариантах модуль 313 управления ключами копирует пустой сертификат, хранящийся в компьютере или коммуникационном терминале. Например, пустой сертификат имеет ограниченный срок действия или использования в зависимости от типа или назначения обслуживания, срока предоставления обслуживания, надежности пользователя и тому подобного. В некоторых вариантах осуществления срок действия пустого сертификата такой же, как срок действия смарт-карты. Кроме того, в некоторых вариантах осуществления изобретения множество пустых сертификатов имеют отличающиеся друг от друга даты истечения срока действия и приемы использования.

[0075] Модуль 314 биометрической аутентификации сравнивает биометрические данные, собранные модулем 311 сбора биометрической информации, с зашифрованными биометрическими данными, хранящимися на смарт-карте. Кроме того, модуль 314 биометрической аутентификации сравнивает биометрические данные, полученные модулем 311 сбора биометрической информации, с биометрическим кодом, вставленным в сертификат открытого ключа, хранящийся в смарт-карте. То есть модуль 314 биометрической аутентификации определяет, соответствуют ли биометрические данные зашифрованным биометрическим данным и биометрическому коду, хранящемуся в смарт-карте, или нет. В некоторых вариантах осуществления изобретения модуль 314 биометрической аутентификации сравнивает собранные биометрические данные либо с одним из наборов зашифрованных биометрических данных, либо с биометрическим кодом, хранящимся в смарт-карте.

[0076] Модуль 315 управления VPN устанавливает и управляет VPN с удаленным объектом, таким как сервер, предоставляющий обслуживание, и обеспечивает сквозное шифрование и участок безопасной передачи. Например, когда модулем 122 биометрической аутентификации определено, что собранные биометрические данные согласуются с зашифрованными биометрическими данными и биометрическим кодом, хранящимся в смарт-карте, модуль 315 управления VPN передает стартовый сигнал туннелирования для установления VPN сервера, предоставляющего сервис, с коммуникационным терминалом. Сигнал запуска туннелирования содержит URL-адрес назначения для установления VPN. Коммуникационный терминал включает в себя терминал открытого обслуживания (ATM, Kiosk, POS, и тому подобное), а также частный коммуникационный терминал (например, мобильный телефон, планшетный ПК, настольный компьютер, ноутбук и тому подобное), и подразумевает охват всех устройств, которые могут связываться с удаленным объектом в коммуникационной сети.

[0077] Когда модуль 312 управления биометрической информацией управляет множеством фрагментов биометрических данных, модуль 315 управления VPN выполнен с возможностью передавать сигнал запуска туннелирования, задавая различные URL-адреса назначения для установления VPN в зависимости от биометрических данных, которые соответствуют реальным биометрическим данным, вводимым посредством

модуля 311 сбора биометрической информации из множества фрагментов сохраненных биометрических данных. URL-адрес назначения принадлежит серверу поставщика услуг, обеспечивающего предоставление различных сервисов, включая обслуживание банковских/кредитных карт, сервис по оплате, сервис электронного государства, облачный сервис, обслуживание, связанное с IoT устройствами, аварийный сервис и тому подобное, пользователю, прошедшему аутентификацию. Такой URL-адрес может быть задан на этапе изготовления смарт-карты, на этапе выдачи сертификата или на этапе генерации закрытого ключа/открытого ключа. Например, URL-адрес вставляется в сертификат открытого ключа, который изначально хранится в смарт-карте, или хранится в той же области хранения, где хранится сертификат открытого ключа. В некоторых вариантах осуществления областью хранения является область в микросхеме, где не допускается изменение данных. В некоторых вариантах, когда на смарт-карте дополнительно выпускается новый сертификат открытого ключа, URL-адрес, связанный с выпускаемым сертификатом открытого ключа, получается вместе с ним или выдается сертификат открытого ключа, в который вставлен связанный с ним URL-адрес. В некоторых вариантах осуществления такой сертификат открытого ключа хранится в области микросхемы, где допускается изменение данных. В некоторых вариантах URL-адрес вставляется в закрытый ключ/открытый ключ введением в состав биометрического кода.

[0078] Кроме того, для уведомления об аварийной ситуации с пользователем могут использоваться специфические биометрические данные из множества фрагментов биометрических данных или специфическая комбинация из множества фрагментов биометрических данных (может быть назначен их порядок). Например, сигнал запуска туннелирования, соответствующий определенным биометрическим данным, конфигурируется так, чтобы вызвать установление VPN с определенным заранее URL-адресом (например, сервером органа полиции и сервером управления безопасностью) для оповещения об аварийной ситуации с пользователем. При такой конфигурации, когда пользователю под воздействием угрозы третьей стороны приходится принудительно выполнять процедуру аутентификации пользователя с помощью смарт-карты 120, пользователь может передавать сигнал аварийной ситуации на сервер органа полиции без обнаружения третьей стороной, используя заранее определенные специфические биометрические данные из множества зарегистрированных фрагментов биометрических данных. Такой сигнал об аварийной ситуации может быть использован позже для обращения по страховке или доказательства при судебном иске.

[0079] При установлении коммуникационного туннеля с сервером, предоставляющим обслуживание, модуль 316, выполняющий процесс аутентификации, передает информацию об аутентификации на основе закрытого ключа, который управляется модулем 313 управления ключом, соответствующему серверу, предоставляющему обслуживание, удостоверяя таким образом пользователя смарт-карты 120 как законного пользователя. Информация об аутентификации описана далее со ссылкой на фиг. 6.

[0080] В некоторых вариантах осуществления изобретения смарт-карта дополнительно включает в себя модуль 317 генерации OTP. Модуль 317 генерации OTP генерирует одноразовый пароль (OTP) способом, заданным организацией, выпускающей смарт-карту 120. В некоторых вариантах осуществления OTP, сгенерированный модулем 317 генерации OTP, отображается на дисплее смарт-карты, так что пользователь смарт-карты 120 может видеть OTP, и модуль 317 генерации OTP выполнен с возможностью передать введенный пользователем OTP модулю 316, выполняющему процесс аутентификации. В некоторых вариантах осуществления одноразовый пароль,

генерируемый модулем 317 генерации OTP, передается непосредственно в модуль 316, выполняющий процесс аутентификации, без отображения на дисплее. OTP, переданный в модуль 316, выполняющий процесс аутентификации, объединяется с информацией об аутентификации на основе сертификата и передается на целевой терминал. Посредством этого процесса смарт-карта 120 может быть проверена (аутентифицирована) на предмет ее выпуска легальной выпускающей организацией. Следует отметить, что в рамках обычной технологии в соответствующей технической области устройство OTP использовалось отдельно от смарт-карты.

[0081] В некоторых вариантах осуществления смарт-карта 120 дополнительно включает в себя модуль 318 сбора информации об устройстве. Модуль 318 сбора информации об устройстве собирает идентификационные данные IoT устройства. Идентификационные данные IoT устройства являются уникальными идентификационными данными, присвоенными IoT устройству во время изготовления, распространения или покупки IoT устройства, и подробно описаны далее со ссылкой на фиг. 6. Модуль 318 сбора информации об устройстве выполнен с возможностью получения идентификационных данных IoT устройства от датчика, встроенного в смарт-карту 120 или коммуникационный терминал 150, или от другого внешнего устройства (например, ATM, Kiosk, POS, считывателя карт или тому подобного), включающего в себя по меньшей мере один датчик.

[0082] На фиг. 4A приведена функциональная схема процедуры регистрации пользователя в соответствии с некоторыми вариантами осуществления настоящего изобретения. Процедура регистрации пользователя, показанная на фиг. 4A, подходит для системы аутентификации пользователя, имеющей конфигурацию, показанную на фиг. 1A. В примере, показанном на фиг. 4A, предполагается, что сертификат открытого ключа заранее сохранен в смарт-карте (например, во время изготовления или выдачи смарт-карты); однако, можно также получить новый сертификат открытого ключа от сервера центра сертификации (CA).

[0083] Сначала коммуникационный терминал собирает биометрические данные пользователя и передает полученные биометрические данные пользователя на смарт-карту (этапы S401 и S402). При сборе биометрических данных используется биометрический датчик, встроенный в коммуникационный терминал, или внешний биометрический датчик, связанный с коммуникационным терминалом. В отличие от примера, показанного на фиг. 4A, в некоторых вариантах осуществления изобретения смарт-карта непосредственно собирает биометрические данные пользователя с помощью встроенного биометрического датчика.

[0084] После сбора биометрических данных пользователя смарт-карта зашифровывает биометрические данные пользователя на основе предварительно сохраненного или предустановленного сертификата открытого ключа (этап S403). То есть смарт-карта зашифровывает биометрические данные в соответствии с алгоритмом шифрования, определенным в сертификате открытого ключа.

[0085] Далее смарт-карта генерирует кодовое значение путем кодирования или маркирования зашифрованных биометрических данных (этап S404). Алгоритм кодирования или маркирования встроен в приложение смарт-карты или определен в сертификате открытого ключа. Например, в некоторых вариантах осуществления изобретения в процессе кодирования или маркирования используется алгоритм хеширования или аналогичный алгоритм, определенный в сертификате открытого ключа. Кодовое значение представляет собой информацию, полученную путем кодирования биометрических данных пользователя на основе сертификата открытого

ключа, и, следовательно, его можно назвать «биометрическим кодом», «биометрической цифровой подписью».

[0086] Затем смарт-карта генерирует пару ключей (открытый ключ и закрытый ключ) помещая биометрический код в EV (расширенной проверки) домен сертификата открытого ключа. То есть биометрический код вставляется в сгенерированные закрытый ключ и открытый ключ. Закрытый ключ хранится в смарт-карте вместе с зашифрованными биометрическими данными для последующего использования в процедуре аутентификации пользователя (этап S405). Хотя это не показано на фиг. 4A, различные добавочные коды, которые генерируются таким же или подобным образом, что биометрический код, могут быть объединены с вышеупомянутым биометрическим кодом в качестве добавочного элемента аутентификации. Например, в домен сертификата открытого ключа может быть вставлен, так же, как и биометрический код, по меньшей мере один из: добавочного кода, полученного из уникальных идентификационных данных, закрепленных за портативным устройством, добавочного кода, полученного из информации о местоположении, указывающей положение, в котором запрашивается аутентификация пользователя, добавочного кода, полученного из уникальных идентификационных данных, закрепленных за пользователем, добавочного кода, полученного из информации, указывающей на характеристики поведения пользователя, или добавочного кода, полученного из идентификационных данных устройства, закрепленных за IoT устройством. Добавочные коды описаны далее со ссылкой на фиг. 6.

[0087] Смарт-карта передает открытый ключ серверу аутентификации (или серверу, предоставляющему обслуживание) через коммуникационный терминал при запросе регистрации пользователя (этап S406). Открытый ключ можно передать с помощью виртуальной частной сети (VPN). Сервер аутентификации регистрирует пользователя и управляет открытым ключом в отдельной безопасной базе данных DB (этапы S407-S408).

[0088] На фиг. 4B приведена функциональная схема процедуры регистрации пользователя в соответствии с некоторыми вариантами осуществления настоящего изобретения. Процедура регистрации пользователя, показанная на фиг. 4B, пригодна для системы аутентификации пользователей, имеющей конфигурацию, показанную на фиг. 1B. Таким образом, коммуникационный терминал, показанный на фиг. 4B, включает в себя персональный коммуникационный терминал (например, мобильный телефон, носимое устройство, такое как часы, очки, кольцо или тому подобное, планшетный ПК, настольный компьютер, ноутбук и тому подобное), и подразумевает охват всех устройств, которые могут связываться с удаленным объектом в коммуникационной сети.

[0089] Коммуникационный терминал запрашивает у сервера центра сертификации (CA) выдачу сертификата открытого ключа для выполнения регистрации пользователя (этап S451). Сервер центра сертификации (CA) выдает сертификат открытого ключа коммуникационному терминалу (этап S452). В отличие от примера, показанного на фиг. 4A, в некоторых вариантах осуществления изобретения сертификат открытого ключа сохраняется в коммуникационном терминале заранее (например, во время изготовления или размещения коммуникационного терминала).

[0090] Затем коммуникационный терминал собирает биометрические данные пользователя (этап S453). При сборе биометрических данных может использоваться встроенный биометрический датчик коммуникационного терминала или биометрический датчик внешнего устройства, связанный с коммуникационным терминалом.

[0091] Далее коммуникационный терминал зашифровывает биометрические данные пользователя с помощью выданного сертификата открытого ключа (этап S454). То есть коммуникационный терминал зашифровывает биометрические данные на основе алгоритма шифрования, определенного в сертификате открытого ключа. Зашифрованные биометрические данные сохраняются в коммуникационном терминале для последующего использования в процедуре аутентификации пользователя.

[0092] Коммуникационный терминал кодирует или маркирует зашифрованные биометрические данные и генерирует кодовое значение (то есть биометрический код) (этап S455). Алгоритм кодирования или маркирования может храниться в приложении коммуникационного терминала или определяться в сертификате открытого ключа. В некоторых вариантах осуществления изобретения в качестве алгоритма кодирования или маркирования может использоваться алгоритм хеширования, определенный в сертификате открытого ключа.

[0093] Затем коммуникационный терминал генерирует пару ключей (открытый ключ и закрытый ключ) путем вставки сгенерированного биометрического кода в домен расширенной проверки (EV) сертификата открытого ключа (этап S456). То есть биометрический код вставляется в сгенерированные закрытый ключ и открытый ключ. Закрытый ключ сохраняется в коммуникационном терминале, чтобы затем использовать его в процедуре аутентификации пользователя. Хотя это не показано на фиг. 4A, другой добавочный код может быть сгенерирован тем же самым или подобным образом, что и для биометрического кода, и добавлен в сертификат открытого ключа в качестве добавочного элемента аутентификации.

[0094] Кроме того, коммуникационный терминал передает открытый ключ серверу аутентификации (или серверу, предоставляющему обслуживание) для запроса регистрации пользователя (этап S457). Открытый ключ можно передать с помощью виртуальной частной сети (VPN). Сервер аутентификации регистрирует пользователя и управляет открытым ключом в отдельной безопасной базе данных (этапы S458-S459).

[0095] На фиг. 5A и 5B представлены схемы форматов сертификатов открытого ключа, применяемых в распределенной системе управления идентификацией в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[0096] Сертификат открытого ключа (например, сертификат X.509, использующий инфраструктуру открытого ключа (PKI) стандарта ITU-T) - это своего рода электронная гарантия, которая предоставляет сторонам сделки возможность доверять друг к другу при осуществлении бизнеса или сделки в сети Интернет. Сертификат открытого ключа может быть выдан центром сертификации, установленным конкретным государственным или финансовым учреждением, частным центром сертификации, производителем продукта или учреждением, предоставляющим обслуживание устройств.

[0097] Примерный формат сертификата открытого ключа без процедуры регистрации пользователя показан на фиг. 5A. Сертификат открытого ключа содержит: версию, серийный номер, алгоритм подписи, выпускающий орган, срок действия, открытый ключ, электронную подпись выпускающего органа и тому подобное. Следует отметить, что домен расширенной проверки (EV) сертификата открытого ключа без процедуры регистрации пользователя является пустым.

[0098] Примерный формат сертификата открытого ключа (открытый ключ/закрытый ключ), сгенерированный сертификатом открытого ключа при процедуре регистрации пользователя, показан на фиг. 5B. В отличие от примера, показанного на фиг. 5A, биометрический код, генерируемый путем кодирования биометрических данных пользователя, вставляется в домен расширенной проверки (EV) сертификата открытого

ключа при процедуре регистрации пользователя или в генерируемый открытый ключ/закрытый ключ. Различные добавочные коды могут быть объединены с биометрическим кодом, сохраняемым в домене EV, в качестве добавочного элемента аутентификации. Подробные сведения о добавочных кодах описаны со ссылкой на фиг. 6.

[0099] В некоторых вариантах осуществления настоящего изобретения могут использоваться сертификаты открытого ключа различных выпускающих органов и различных форматов. Соответственно, формат сертификата открытого ключа, в который вставлен биометрический код, не ограничивается примерами, показанными на фиг. 5A и 5B, а расширенный домен сертификата открытого ключа, в который вставлен биометрический код, не ограничивается доменом EV.

[00100] На фиг. 6 представлена схема примерного формата кода, сохраняемого в EV домене открытого ключа/закрытого ключа, показанного на фиг. 5B, и примерный формат информации аутентификации, передаваемой со смарт-карты.

[00101] Как описано выше, только биометрический код, генерируемый просто кодированием биометрических данных пользователя, может быть сохранен в EV домене открытого ключа/закрытого ключа (см. фиг. 6(a)), и код, выполненный путем объединения, по меньшей мере, одного из различных добавочных кодов с биометрическим кодом, также может быть сохранен. Например, в некоторых вариантах добавочный код (то есть код устройства), закодированный (маркированный) из идентификационных данных IoT устройства пользователя, может быть соединен с биометрическим кодом (см. фиг. 1). 6(b) и (c)). Идентификационные данные IoT устройства - это уникальные идентификационные данные, присвоенные каждому IoT устройству во время изготовления, распространения или покупки устройства. Идентификационные данные IoT устройства содержат номер устройства, информацию о выпуске, серийный номер, электронный код продукта (EPC), универсальный код продукта (UPC), физически неклонируемую функцию (PUF), общий идентификационный номер (GSIN) отгрузки, MAC-адрес, и тому подобное. Идентификационные данные IoT устройства могут быть собраны со штрих-код и QR-кода, напечатанных на IoT-устройстве или с электронного элемента, встроенного в IoT устройство. Использование кода устройства описано далее со ссылкой на фиг. 8.

[00102] В некоторых вариантах осуществления изобретения добавочный код, полученный кодированием идентификационных данных смарт-карты или коммуникационного терминала, в которых хранится сертификат открытого ключа, может быть объединен с биометрическим кодом (см. фиг. 6(d)). Идентификационные данные смарт-карты или коммуникационного терминала, в которых хранится сертификат открытого ключа, содержит, например, значение криптографической хэш-функции, физически неклонируемую функцию (PUF), номера платежных карт и тому подобное.

[00103] В некоторых вариантах осуществления изобретения добавочный код, полученный кодированием (или маркированием) из специфических идентификационных данных (например, номера социального страхования, личных идентификационных данных или персонального номера доступа), присвоенных пользователю государством или банком, или из информации, относящейся к характеристикам поведения пользователя (например, нажатия клавиш или динамической подписи), может быть объединен с биометрическим кодом (см. фиг. 6(e) и (f)). Информация, относящаяся к характеристикам поведения пользователя, может быть получена с помощью сенсорного экрана смарт-карты или коммуникационного терминала.

[00104] В некоторых вариантах осуществления изобретения добавочный код,

полученный кодированием (или маркированием) из информации о местоположении коммуникационного терминала (или смарт-карты) (например, от глобальной системы позиционирования (GPS), от группы по наблюдениям Земли (GEO)), может быть объединен с биометрическим кодом. Этот добавочный код может применяться для обнаружения, защиты от кражи или утери информации или устройства или доказательства незаконной транзакции, путем его учета в качестве добавочного элемента аутентификации, независимо от того, выполняется ли транзакция в месте, отличном от обычного местоположения транзакции (например, финансовая транзакция, деятельность по обслуживанию кредитов, финансовые расчеты, платежный сервис и оплата), или нет.

[00105] Кроме того, с биометрическим кодом может быть связано множество добавочных кодов (см. фиг. 6(g)-(i)). Фиг. 6(j) представляет код, полученный путем объединения множества добавочных кодов с биометрическим кодом. В объединенном коде длины биометрического кода и добавочных кодов могут быть одинаковыми или отличаться друг от друга.

[00106] Практически тот же алгоритм, что и для генерирования биометрического кода, может быть применен как алгоритм для генерирования добавочных кодов. Кроме того, данные, зашифрованные в процессе генерации добавочных кодов (например, зашифрованная динамическая подпись), могут быть сохранены в смарт-карте или коммуникационном терминале вместе с закрытым ключом. Зашифрованные данные, сохраненные в смарт-карте или коммуникационном терминале, могут использоваться в качестве добавочного средства аутентификации для первичной аутентификации пользователя (на основе биометрического соответствия), выполняемой на смарт-карте или в коммуникационном терминале.

[00107] Фиг. 6(j) представляет код, содержащийся в информации об аутентификации, передаваемой серверу, предоставляющему обслуживание, в ходе процедуры аутентификации пользователя. То есть, информация аутентификации содержит код, вставленный в закрытый ключ (объединенный с ним). Этот аспект подробно описан далее со ссылкой на фиг. 7A.

[00108] В частности, код, вставленный в закрытый ключ/открытый ключ, и информация аутентификации, передаваемая от смарт-карты, имеют различные форматы в соответствии с примером применения и/или степенью защиты, который не ограничивается несколькими расстановками или комбинациями, показанными на фиг. 6. Кроме того, могут быть дополнительно использованы элементы другие, чем элементы аутентификации, показанные на фиг. 6.

[00109] На фиг. 7A приведена структурная схема процедуры аутентификации пользователя в соответствии с некоторыми вариантами осуществления настоящего изобретения. Процедура регистрации пользователя, показанная на фиг. 7A, пригодна для системы аутентификации пользователей, которая имеет конфигурацию, показанную на фиг. 1A.

[00110] Сначала коммуникационный терминал получает биометрические данные пользователя и передает полученные биометрические данные пользователя на смарт-карту (этапы S701-S702). При получении биометрических данных используется биометрический датчик, встроенный в коммуникационный терминал, или внешний биометрический датчик, связанный с коммуникационным терминалом. В отличие от примера, показанного на фиг. 7A, в некоторых вариантах осуществления изобретения смарт-карта непосредственно собирает биометрические данные пользователя с помощью встроенного биометрического датчика.

[00111] Затем смарт-карта сравнивает полученные биометрические данные с зашифрованными биометрическими данными, хранящимися в смарт-карте, и/или биометрическим кодом, вставленным в закрытый ключ, хранящийся в смарт-карте (этап S703). То есть смарт-карта определяет, соответствуют ли собранные биометрические данные зашифрованным биометрическим данным и/или биометрическому коду, хранящемуся в смарт-карте.

[00112] Если установлено, что собранные биометрические данные соответствуют зашифрованным биометрическим данным и биометрическому коду, хранящемуся в смарт-карте, смарт-карта передает информацию об аутентификации на основе закрытого ключа на сервер, предоставляющий обслуживание, через коммуникационный терминал (этап S704). Информация об аутентификации может быть передана с помощью виртуальной частной сети (VPN). Например, смарт-карта передает сигнал запуска туннелирования для установления VPN с сервером, предоставляющим обслуживание, коммуникационному терминалу, и коммуникационный терминал устанавливает VPN между сервером, предоставляющим обслуживание, и смарт-картой в ответ на сигнал запуска туннелирования. Смарт-карта передает информацию об аутентификации серверу, предоставляющему обслуживание, через установленную VPN. Сигнал запуска туннелирования содержит URL-адрес назначения для установления VPN.

[00113] Сервер, предоставляющий обслуживание, запрашивает сервер аутентификации о проверке принятой информации аутентификации (этап S705). Сервер аутентификации проверяет информацию аутентификации с помощью зарегистрированного открытого ключа. Сервер, предоставляющий обслуживание, завершает аутентификацию пользователя в соответствии с результатом проверки сервером аутентификации (этапы S706-S708).

[00114] Информация об аутентификации, передаваемая серверу, предоставляющему обслуживание, генерируется на основе кода, вставленного в закрытый ключ, хранящийся на смарт-карте (см. фиг. 6(a)-(i)). Например, информация об аутентификации содержит биометрический код, вставленный в домен EV сертификата открытого ключа, или сам объединенный код. В некоторых вариантах осуществления информация об аутентификации дополнительно содержит OTP, генерируемый программируемым OTP генератором, встроенным в смарт-карту, так же как и код, вставленный в EV домен сертификата (см. фиг. 6(j)). В некоторых вариантах осуществления изобретения каждый из элементов аутентификации (биометрической код, OTP, PUF и тому подобное) передается в отдельной форме, а в некоторых вариантах, каждый из элементов аутентификации передается как единый фрагмент объединенных данных аутентификации.

[00115] В некоторых вариантах осуществления информация об аутентификации, передаваемая серверу, предоставляющему обслуживание, дополнительно содержит уникальную информацию для подтверждения действия пользователя по аутентификации. В некоторых вариантах уникальная информация приводится в форме штрих-кода, электронной подписи пользователя и тому подобного, что позволяет провести аутентификацию пользователя. Кроме того, такой штрих-код и электронная подпись могут быть предоставлены в форме, которая может быть выведена в печатном виде. Действие по аутентификации с помощью смарт-карты может повысить надежность договора между сторонами, допуская печать квитанции или выписки из счета в виде штрихкода или подписи. В некоторых вариантах осуществления информация об аутентификации, передаваемая серверу, предоставляющему обслуживание, дополнительно содержит сведения о времени передачи информации об аутентификации. В некоторых вариантах информация об аутентификации, передаваемая серверу,

предоставляющему обслуживание, дополнительно содержит информацию о времени (то есть отметку времени) регистрации пользователя (например, время генерации закрытого ключа/открытого ключа или время завершения регистрации пользователя на сервере аутентификации).

[00116] С помощью этой процедуры аутентификации пользователя можно обеспечить взаимодействие с пользователем, сравнимое с обычной технологией. Например, предположим, что установлено соединение с системой интернет-банкинга с помощью смарт-карты. В этом случае обычный этап ввода идентификатора пользователя (ID) для доступа к серверу, предоставляющему обслуживание и обеспечивающему интернет-банкинг, заменяется этапом установления коммуникационного туннеля на основе биометрических данных пользователя. Далее, обычный этап ввода пароля пользователя заменяется этапом передачи информации аутентификации, содержащей код, вставленный в закрытый ключ через установленный коммуникационный туннель. Кроме того, обычный этап ввода пароля сертификата открытого ключа заменяется этапом сравнения биометрических данных пользователя с соответствующей информацией, содержащейся в сертификате открытого ключа. То есть, согласно некоторым вариантам осуществления настоящего изобретения, этапы ввода сертификата и пароля, требуемые сервером, предоставляющим обычное обслуживание, могут быть опущены. Таким образом, выполняя процесс туннелирования и аутентификации с помощью смарт-карты, можно обойтись единственным указанием с использованием биометрических данных.

[00117] Кроме того, при многофакторной аутентификации по традиционной технологии, всеми элементами аутентификации, в том числе ID, паролем, паролем сертификата, OTP и тому подобным, управляют, соответственно, как отдельными элементами аутентификации. Наоборот, в соответствии с некоторыми вариантами осуществления настоящего изобретения, зашифрованные биометрические данные пользователя, биометрический код и добавочный код используются в качестве информации аутентификации в объединенной форме. Вследствие этого, может быть успешно выполнена многофакторная аутентификация с более сильной защитой, чем одношаговая, то есть распределенная аутентификация «нажми и заплати».

[00118] На фиг. 7B приведена структурная схема процедуры аутентификации пользователя в соответствии с некоторыми вариантами осуществления настоящего изобретения. Процедура регистрации пользователя, показанная на фиг. 7B, пригодна для системы аутентификации пользователя, имеющей конфигурацию, показанную на фиг. 1B.

[00119] Сначала коммуникационный терминал собирает биометрические данные пользователя (этап S751). При сборе биометрических данных используется биометрический датчик, встроенный в коммуникационный терминал, или внешний биометрический датчик, связанный с коммуникационным терминалом.

[00120] Затем коммуникационный терминал сравнивает полученные биометрические данные с зашифрованными биометрическими данными, хранящимися в коммуникационном терминале, и/или биометрическим кодом, вставленным в закрытый ключ, хранящийся в коммуникационном терминале (этап S752). То есть коммуникационный терминал определяет, соответствуют ли полученные биометрические данные зашифрованным биометрическим данным и/или биометрическому коду, хранящемуся в коммуникационном терминале.

[00121] Если установлено, что полученные биометрические данные соответствуют зашифрованным биометрическим данным и биометрическому коду, хранящемуся в коммуникационном терминале, коммуникационный терминал передает информацию

аутентификации на основе закрытого ключа на сервер, предоставляющий обслуживание (этап S753). Информация аутентификации может быть передана с помощью виртуальной частной сети (VPN). Например, коммуникационный терминал устанавливает VPN между сервером, предоставляющим обслуживание, и смарт-картой, и смарт-карта передает информацию аутентификации серверу, предоставляющему обслуживание, через установленную VPN.

[00122] Сервер, предоставляющий обслуживание, запрашивает у сервера аутентификации проверку полученной информации аутентификации (этап S754). Сервер аутентификации проверяет данные проверки информации аутентификации с помощью зарегистрированного открытого ключа. Сервер, предоставляющий обслуживание, завершает аутентификацию пользователя в соответствии с результатом проверки, проведенной сервером аутентификации (этапы S755-S757).

[00123] В приведенном выше описании описан способ аутентификации пользователя на основе закрытого ключа/открытого ключа, в который вставлен биометрический код. В некоторых вариантах осуществления настоящего изобретения, описанных далее, биометрический код пользователя связан с данными идентификации IoT устройства и используется для управления и контроля IoT устройства. Некоторые варианты осуществления, относящиеся к IoT устройствам, описаны ниже со ссылкой на фиг. 8, 9, 10A, и 10B.

[00124] На фиг. 8A и 8B приведены схемы конфигурации системы для управления пользователем IoT устройством в распределенной среде в соответствии с некоторыми вариантами осуществления настоящего изобретения.

[00125] Как показано на фиг. 8A, IoT сеть 800 включает в себя множество IoT устройств 850, причем каждое имеет функцию проводной/беспроводной связи. Как описано выше, смарт-карта 810 выполнена с возможностью вставлять добавочный код (то есть код устройства), генерируемый при кодировании идентификационных данных IoT устройства пользователя, а также биометрический код при генерации закрытого ключа/открытого ключа из сертификата открытого ключа. Это позволяет подтвердить отношения собственности между пользователем и IoT устройством путем сопоставления биометрического кода пользователя с данными идентификации IoT устройства.

[00126] В соответствии с некоторыми вариантами осуществления настоящего изобретения, смарт-карта 810 генерирует закрытый ключ и открытый ключ, в которые вставлены биометрический код и код устройства, сохраняет закрытый ключ и передает открытый ключ соответствующему IoT устройству 850. Смарт-карта 810 передает информацию аутентификации на основе закрытого ключа IoT устройству 850, и IoT устройство 850 выполняет аутентификацию пользователя (владельца), проверяя информацию аутентификации с помощью открытого ключа.

[00127] В сети, которая покрывает заданную область, такую как предприятие, здание, бизнес-сектор, жилище, автомобиль или тому подобное, может быть IoT устройство (например, телеприставка, точка доступа и тому подобное в домашней сети), которое управляет (регистрирует, отслеживает и контролирует) различными IoT устройствами, подключенными к сети, то есть централизованный контроллер 830. Централизованный контроллер 830 дополнительно выполнен с возможностью выполнения роли пользовательского интерфейса и имеет дополнительную функцию сочетания функций IoT устройств 850 для предоставления комплексного обслуживания. В этом случае смарт-карта 810 используется для регистрации IoT устройства 850 и аутентификации пользователя (владельца) для удаленного управления IoT устройством 850 по сети путем передачи открытого ключа, соответствующего каждому IoT устройству 850, к

централизованному контроллеру 830.

[00128] Кроме того, смарт-карта 810 используется для регистрации IoT устройства 850 и аутентификации пользователя (владельца) для удаленного управления IoT устройством 850 по сети, путем передачи открытого ключа серверу 840 провайдера IoT обслуживания, который предоставляет IoT обслуживание.

[00129] Кроме того, смарт-карта 810 используется для аутентификации пользователя (владельца) для регистрации, изменения и передачи собственности на IoT устройство путем передачи открытого ключа на сервер производителя/продавца IoT устройства 850.

[00130] Кроме того, смарт-карта может использоваться как единый центр дистанционного управления для управления каждым из IoT устройств 850 посредством передачи открытых ключей, связанных с IoT устройствами, коммуникационному терминалу 820 (например, мобильному телефону) и посредством коммуникационного терминала 820, используя открытые ключи IoT устройств. Например, пользователь выполняет процедуру аутентификации пользователя (первую аутентификацию) на коммуникационном терминале 820 с помощью закрытого ключа, хранящегося на смарт-карте, и при успешной первой аутентификации, выполняет управление отдельным IoT устройством или централизованным контроллером 830 с помощью открытого ключа, хранящегося в коммуникационном терминале 820, не будучи связанным со смарт-картой.

[00131] В некоторых вариантах осуществления настоящего изобретения, комбинация характерных фрагментов биометрических данных может быть использована для переустановки IoT устройства или управления важной функцией IoT устройства. Например, закрытый ключ/открытый ключ, в который вставлена информация кода, полученного из комбинации характерных фрагментов биометрических данных, может быть использован для переустановки IoT устройства или управления важной функцией IoT устройства, когда IoT устройство находится в неисправном состоянии, не управляется или тому подобное.

[00132] Функции смарт-карты 810, показанная на фиг. 8A, может быть введена в состав коммуникационного терминала 820. То есть, в соответствии с некоторыми осуществлениями настоящего изобретения, как показано на фиг. 8B, коммуникационный терминал 860 генерирует закрытый ключ и открытый ключ, в который вставляются биометрический код и код устройства. Коммуникационный терминал 860 сохраняет закрытый ключ и передает открытый ключ соответствующему IoT устройству 850, серверу 840 провайдера IoT обслуживания, серверу производителя/продавца IoT устройства и централизованному контроллеру 830.

[00133] Нижеследующее описание поясняет, со ссылкой на фиг. 9A-10B, процедуру регистрации и аутентификации пользователя (владельца) с использованием централизованного контроллера IoT устройств. Следует понимать, что та же/подобная процедура может быть выполнена с серверами индивидуальных IoT устройств и IoT провайдеров обслуживания и с серверами производителей /продавцов IoT устройств.

[00134] На фиг. 9A приведена структурная схема процедуры регистрации пользователя устройства в соответствии с некоторыми вариантами осуществления настоящего изобретения. Процедура регистрации пользователя на фиг. 9A подходит для системы аутентификации пользователя устройства, имеющей конфигурацию, показанную на фиг. 8A.

[00135] В дополнительной предварительной процедуре смарт-карта 810 может использовать закрытый ключ с заранее сохраненными зашифрованными

биометрическими данными и/или биометрическим кодом, вставленными для выполнения биометрической аутентификации пользователя в процедуре регистрации пользователя устройства. Другими словами, смарт-карта 810 может быть выполнена так, чтобы разрешить процедуру регистрации пользователя устройства исключительно для зарегистрированных пользователей.

[00136] Сначала коммуникационный терминал 820 запрашивает биометрические данные пользователя и передает полученные биометрические данные пользователя на смарт-карту 810 (S901-S902). Здесь при сборе биометрических данных может быть выбран встроенный биометрический датчик коммуникационного терминала 820 или биометрический датчик, предусмотренный во внешнем устройстве, соединенном с коммуникационным терминалом 820. В отличие от иллюстрации на фиг. 9A, в других вариантах осуществления может быть смарт-карта 810, содержащая биометрический датчик для немедленного получения биометрических данных пользователя.

[00137] Смарт-карта 810 зашифровывает биометрические данные пользователя с помощью заранее сохраненного открытого ключа и кодирует (или маркирует) зашифрованные биометрические данные для генерации биометрического кода (S903). Алгоритмы шифрования и кодирования (или маркирования) могут быть встроены в приложение смарт-карты 810, или они могут быть указаны в сертификате открытого ключа.

[00138] Затем смарт-карта 810 собирает идентификационные данные устройства, закрепленные за IoT устройством, через коммуникационный терминал (S904-S905). Здесь для сбора идентификационных данных устройства может быть выбран встроенный биометрический датчик коммуникационного терминала 820 или биометрический датчик, предусмотренный во внешнем устройстве, связанном с коммуникационным терминалом 820. В отличие от иллюстрации на фиг. 9A, в других вариантах осуществления может иметься смарт-карта 810, содержащая биометрический датчик для немедленного получения идентификационных данных устройства.

[00139] Далее, тем же способом, какой описан выше для биометрического кода, или аналогичным, смарт-карта 810 генерирует код устройства из идентификационных данных устройства (S906). А именно, смарт-карта 810 зашифровывает идентификационные данные устройства и кодирует или маркирует зашифрованные идентификационные данные устройства для генерирования кода устройства.

[00140] Затем смарт-карта 810 вставляет биометрический код и код устройства в домен расширенной проверки (EV) сертификата открытого ключа для генерирования пары ключей (открытого ключа и закрытого ключа). Другими словами, сгенерированные закрытый ключ и открытый ключ содержат вставленный в них биометрический код и код устройства. Вставленные биометрический код и код устройства в закрытом ключе и открытом ключе могут быть сформированы таким образом, чтобы они были объединены. Закрытый ключ хранится в смарт-карте 810 вместе с зашифрованными биометрическими данными (S907). Хотя это не показано на фиг. 9A, для генерации закрытого ключа и открытого ключа могут использоваться другие добавочные коды, генерируемые тем же или аналогичным способом, что и биометрический код. Такие добавочные коды могут быть добавлены к EV домену сертификата открытого ключа в качестве добавочного фактора аутентификации.

[00141] Затем смарт-карта 810 действует через коммуникационный терминал, обеспечивая открытый ключ для централизованного контроллера, а также запрашивая регистрацию пользователя устройства (S908). Передача открытого ключа может происходить через виртуальную частную сеть (VPN). Централизованный контроллер

830 регистрирует пользователя устройства и сохраняет открытый ключ в отдельной защищенной DB (S909-S910).

[00142] На фиг. 9B приведена функциональная схема процедуры регистрации пользователя устройства в соответствии с некоторыми вариантами осуществления настоящего изобретения. Процедура регистрации пользователя на фиг. 9B подходит для системы аутентификации пользователя устройства с такой конфигурацией, какая показана на фиг. 8B.

[00143] В дополнительной предварительной процедуре коммуникационный терминал 860 может использовать закрытый ключ с заранее сохраненными зашифрованными биометрическими данными и/или биометрическим кодом, вставленными для выполнения биометрической аутентификации пользователя в процедуре регистрации пользователя устройства. Другими словами, коммуникационный терминал 860 может быть выполнен так, чтобы разрешить регистрацию пользователя устройства исключительно для зарегистрированных пользователей.

[00144] Сначала коммуникационный терминал 860 собирает биометрические данные пользователя (S951-S952). Здесь при сборе биометрических данных может быть выбран встроенный биометрический датчик коммуникационного терминала 860 или биометрический датчик, предусмотренный во внешнем устройстве, связанном с коммуникационным терминалом 860.

[00145] Коммуникационный терминал 860 зашифровывает биометрические данные пользователя с использованием предварительно сохраненного сертификата открытого ключа и кодирует (или маркирует) зашифрованные биометрические данные для генерации биометрического кода (S953). Алгоритмы шифрования и кодирования (или маркирования) могут быть встроены в приложение смарт-карты или они могут быть указаны в сертификате открытого ключа.

[00146] Затем коммуникационный терминал 860 собирает идентификационные данные устройства, закрепленные за IoT устройством (S954-S955). Здесь при сборе идентификационных данных устройства может быть выбран встроенный биометрический датчик коммуникационного терминала или биометрический датчик, предусмотренный во внешнем устройстве, связанном с коммуникационным терминалом.

[00147] Далее, тем же способом, который описан выше для биометрического кода, или аналогичным, коммуникационный терминал 860 генерирует код устройства из идентификационных данных устройства (S956). А именно, коммуникационный терминал 860 шифрует идентификационные данные устройства и кодирует или маркирует зашифрованные идентификационные данные устройства для создания кода устройства.

[00148] Затем коммуникационный терминал 860 вставляет биометрический код и код устройства в EV домен сертификата открытого ключа для генерации пары ключей (открытого ключа и закрытого ключа). Другими словами, сгенерированные закрытый ключ и открытый ключ содержат биометрический код и код устройства. Вставленные биометрический код и код устройства в закрытом ключе и открытом ключе могут быть сформированы таким образом, чтобы они были объединены. Закрытый ключ хранится в коммуникационном терминале 860 вместе с зашифрованными биометрическими данными (S957). Хотя это не показано на фиг. 9A, другие добавочные коды, генерируемые тем же или аналогичным способом, что и биометрический код, могут использоваться для генерации закрытого ключа и открытого ключа. Такие добавочные коды могут быть добавлены к домену EV сертификата открытого ключа в качестве добавочного фактора аутентификации.

[00149] Затем коммуникационный терминал 860 действует через линии связи,

обеспечивая открытый ключ для централизованного контроллера, а также запрашивая регистрацию пользователя устройства (S958). Передача открытого ключа может происходить через VPN. Централизованный контроллер 830 регистрирует пользователя устройства и сохраняет открытый ключ в отдельной защищенной DB (S959-S960).

[00150] На фиг. 9A и 9B проиллюстрировано, что при процедуре регистрации пользователя устройства генерируется новая пара ключей (закрытый ключ, открытый ключ) независимо от закрытого ключа, ранее сгенерированного и хранящегося в смарт-карте 810 или коммуникационном терминале 860. Однако в других вариантах осуществления новая пара ключей (закрытый ключ, открытый ключ) может быть сгенерирована путем дополнительного помещения кода устройства в предварительно сохраненный закрытый ключ.

[00151] На фиг. 10A приведена структурная схема процедуры аутентификации пользователя устройства в соответствии с некоторыми вариантами осуществления настоящего изобретения. Процедура регистрации пользователя на фиг. 10A подходит для системы аутентификации пользователя устройства с конфигурацией, подобной показанной на фиг. 8A.

[00152] Сначала коммуникационный терминал 820 собирает биометрические данные пользователя и передает собранные биометрические данные пользователя на смарт-карту 810 (S1001-S1002). Здесь при сборе биометрических данных может быть выбран встроенный биометрический датчик коммуникационного терминала 820 или внешний биометрический датчик, связанный с коммуникационным терминалом 820. В отличие от иллюстрации фиг. 10A, в других вариантах осуществления может иметься смарт-карта 810, содержащая биометрический датчик для немедленного получения биометрических данных пользователя.

[00153] Затем смарт-карта 810 сравнивает полученные биометрические данные с предварительно сохраненными зашифрованными биометрическими данными в смарт-карте 810 и/или с биометрическим кодом, содержащимся в предварительно сохраненном на смарт-карте 810 закрытым ключе (S1003). Другими словами, смарт-карта 810 определяет, совпадает ли собранная реальная биометрическая информация с предварительно сохраненными зашифрованными биометрическими данными и/или биометрическим кодом.

[00154] Если собранная реальная биометрическая информация соответствует предварительно сохраненным зашифрованным биометрическим данным и/или биометрическому коду, смарт-карта 810 передает информацию аутентификации на основе закрытого ключа централизованному контроллеру 830 (S1004). Передача информации аутентификации может происходить через VPN. Например, смарт-карта 810 передает стартовый сигнал туннелирования для открытия VPN централизованного контроллера 830 с терминалом 820, который, в свою очередь, открывает VPN между централизованным контроллером 830 и смарт-картой 810, которая затем отправляет информацию аутентификации через открытую VPN к централизованному контроллеру 830.

[00155] Централизованный контроллер 830 проверяет полученную информацию об аутентификации, используя уже зарегистрированный открытый ключ, и завершает аутентификацию пользователя устройства (S1005-S1007) в зависимости от исхода проверки. В некоторых вариантах осуществления централизованный контроллер 830 может запрашивать сервер 840, предоставляющий IoT обслуживание или сервер аутентификации (не показан), чтобы проверить информацию об аутентификации, полученную от смарт-карты 810, для завершения аутентификации пользователя

устройства в соответствии с результатом проверки.

[00156] На фиг. 10B приведена структурная схема процедуры аутентификации пользователя устройства в соответствии с некоторыми вариантами осуществления настоящего изобретения. Процедура регистрации пользователя на фиг. 10B подходит для системы аутентификации пользователя устройства с конфигурацией, показанной на фиг. 8B.

[00157] Сначала коммуникационный терминал 860 собирает биометрические данные пользователя (S1051-S1052). Здесь при сборе биометрических данных может быть выбран встроенный биометрический датчик коммуникационного терминала 860 или биометрический датчик, предусмотренный во внешнем устройстве, связанном с коммуникационным терминалом 860.

[00158] Затем коммуникационный терминал 860 сравнивает собранные биометрические данные с предварительно сохраненными зашифрованными биометрическими данными и/или биометрическим кодом, содержащимся в предварительно сохраненном закрытом ключе (S1053). Другими словами, коммуникационный терминал 860 определяет, соответствует ли собранная реальная биометрическая информация предварительно сохраненным зашифрованным биометрическим данным и/или биометрическому коду.

[00159] Если собранная реальная биометрическая информация соответствует предварительно сохраненным зашифрованным биометрическим данным и/или биометрическому коду, коммуникационный терминал 860 передает информацию аутентификации на основе закрытого ключа централизованному контроллеру 830 (S1054). Передача информации аутентификации может производиться через VPN. Например, коммуникационный терминал 860 пересылает информацию аутентификации через открытую VPN к централизованному контроллеру 830.

[00160] Централизованный контроллер 830 проверяет полученную информацию аутентификации, используя уже зарегистрированный открытый ключ, и завершает аутентификацию пользователя устройства (S1055-1057) в зависимости от исхода проверки. В некоторых вариантах осуществления централизованный контроллер 830 может запрашивать сервер 840, предоставляющий IoT обслуживание, или сервер аутентификации (не показан), чтобы проверить информацию аутентификации для завершения аутентификации пользователя устройства в соответствии с результатом проверки.

[00161] На фиг. 11 представлена схема, иллюстрирующая концепцию распределенной системы аутентификации, соответствующую онлайн/оффлайн среде.

[00162] Всякая распределенная аутентификация касается аутентификации в режиме онлайн, но сетевая среда развивающихся стран не обеспечивает весь регион интернетом или минимальными средствами коммуникации. Кроме того,

землетрясение/тайфун/наводнение/сбои энергопитания/тяжелый снег или такого рода бедствия могут временно вызвать неисправности в онлайн среде. Для преодоления этих временных/постоянных ограничений необходимо надлежащим образом дополнить систему аутентификации на основе онлайн сетевой среды. Например, терминалам обслуживания (или открытым терминалам), таким как ATM, POS и kiosk лучше позволить в наименьшем размере снятие наличных или оплату даже в офлайн среде. В качестве другого примера, даже если интеллектуальная домашняя сеть временно становится офлайн средой, необходимо разрешить ограниченный доступ к централизованному контроллеру, который обеспечивает комплексное управление домашними IoT устройствами. В качестве еще одного примера, смарт-карта имеет сетевую связь с

множеством датчиков или IoT устройств для таких функций, как эксплуатация беспилотного транспортного средства, автоматическое вождение, информирование о местоположении и навигация. Даже когда такой смарт-автомобиль переходит в офлайн режим, необходимо выполнить авторизацию в ограниченных пределах относительно онлайн сетевой среды.

[00163] Настоящее изобретение в некоторых вариантах осуществления представляет способ аутентификации пользователя, который может предоставить некоторое ограниченное обслуживание (например, вывод наличных, оплата покупки продуктов питания, управление доступом и так далее) с ограниченным электрическим питанием в офлайн среде с помощью использования некоторых из различных средств аутентификации, таких как биометрические данные онлайн режима (биометрический код), PKI, OTP и так далее. В соответствии с одним вариантом осуществления настоящего изобретения, сервер, предоставляющий обслуживание, предоставляет пользователю после регистрации пользователя определенные учетные данные или токен, которые могут быть использованы для аутентификации пользователя в офлайн среде. Например, учетными данными может быть модифицированный открытый ключ, производный от открытого ключа, который принят пользователем в процедуре регистрации пользователя, или получен от смарт-карты или коммуникационного терминала.

[00164] На фиг. 12 приведена структурная схема процедуры аутентификации пользователя в офлайн среде, в соответствии с некоторыми вариантами осуществления настоящего изобретения. Фиг. 11 дана в предположении использования смарт-карты, но по существу та же процедура применяется при использовании коммуникационного терминала (например, смартфона) вместо смарт-карты.

[00165] Сначала, в офлайн среде, открытый терминал (например, ATM, POS, централизованный контроллер и так далее) собирает биометрические данные пользователя и передает собранные биометрические данные на смарт-карту (S1201-S1202). Здесь при получении биометрических данных может быть выбран встроенный биометрический датчик открытого терминала или внешний биометрический датчик, связанный с открытым терминалом. В отличие от иллюстрации фиг. 12, другие варианты осуществления могут иметь смарт-карту, содержащую биометрический датчик, чтобы немедленно получить биометрические данные пользователя.

[00166] Затем смарт-карта сравнивает собранные биометрические данные с предварительно сохраненными зашифрованными биометрическими данными в смарт-карте и/или с содержащимся в заранее сохраненном в закрытом ключе на смарт-карте (S1203) биометрическим кодом. Другими словами, смарт-карта определяет, соответствует ли собранная реальная биометрическая информация предварительно сохраненным зашифрованным биометрическим данным и/или биометрическому коду.

[00167] Если собранная реальная биометрическая информация соответствует предварительно сохраненным зашифрованным биометрическим данным и/или биометрическому коду, смарт-карта передает централизованному контроллеру информацию об аутентификации на основе закрытого ключа и информацию об аутентификации на основе измененного открытого ключа, заранее предоставленного сервером, предоставляющим обслуживание (S1204).

[00168] Открытый терминал в офлайн среде выполняет авторизацию в более ограниченных пределах по сравнению с онлайн средой без запроса сервера, предоставляющего обслуживание, о проверке полученной информации об аутентификации. Другими словами, разрешается определенный ограниченный набор сервисов/транзакций/доступа. В некоторых вариантах осуществления, открытый

терминал может также проверить, были ли коды проверки, вставленные в полученную информацию аутентификации, созданы на основе того же сертификата открытого ключа.

[00169] Соответствующая информация о транзакциях (то есть история транзакций или предоставления услуг и соответствующая информация об аутентификации) хранится в защищенной зоне, содержащей защищенный элемент смарт-карты и/или открытого терминала, для будущего расчета, который будет выполняться в режиме онлайн (S1205). Кроме того, зашифрованные данные транзакции могут храниться с использованием закрытого ключа/открытого ключа.

[00170] При возвращении в онлайн среду, открытый терминал передает сохраненную информацию о транзакции на сервер, предоставляющий обслуживание (S1206). Сервер, предоставляющий обслуживание, проверяет информацию об аутентификации, содержащуюся в информации о транзакции, через сервер аутентификации, и формирует историю транзакций, которая включается в информацию о транзакциях на основе результата проверки (S1207-1209).

[00171] На фиг. 13 приведена таблица примерной области применения, в которой могут быть применены варианты осуществления настоящего изобретения.

[00172] Аутентификация пользователя может выбирать композитные способы аутентификации, но предполагается использовать смарт-карту последовательно интегрированную с информацией из различных приложений, таких как кредитная карта + национальный электронный ID + электронный паспорт + водительское удостоверение.

[00173] Как показано в таблице на фиг. 13, применяемые приложения из вариантов осуществления настоящего изобретения могут быть распределены на четыре основных раздела.

[00174] Раздел финансов и идентификации представляет аутентификацию пользователя, связанную с финансовыми транзакциями и разновидностями идентификации в онлайн/офлайн режиме. Для применения в этих областях смарт-карта (или коммуникационный терминал) могут дополнительно содержать различную информацию по таким инструментам как кредитная карта/дебетовая карта/кибер-деньги/электронный кошелек/цифровой купон/финансовые данные/ значение криптографических хэш-функций/национальный ID/водительское удостоверение/ медицинская информация/пациенты/электронное голосование/пенсия/ уникальные идентификационные данные и так далее. Некоторые из вышеперечисленных сведений могут быть в виде данных, встроенных в EV домен сертификата открытого ключа для соответствующего сервиса. Например, EV домен сертификата открытого ключа для использования при применении национального электронного ID может иметь идентификационные данные, которые однозначно закреплены за человеком (например, регистрационный номер резидента, номер социального страхования и так далее). Кроме того, некоторые сведения могут заранее храниться в той же области, что и сертификат открытого ключа для соответствующего сервиса.

[00175] Раздел физического доступа представляет собой область применения для целей, например, управления доступом посетителей, где смарт-карта (или коммуникационный терминал) может служить ID знаком или картой доступа. Закрытый ключ/открытый ключ для использования в этой области применений может иметь добавленную информацию о местоположении (например, GEO, GIS, GPS информацию) или код, добавленный при ее кодировании (или маркировании). Добавочная информация о местоположении или код может использоваться в качестве добавочного фактора аутентификации для обнаружения фальсификации, подделанного доступа и так далее.

[00176] Раздел единого входа (SSO раздел; объединенная аутентификация) это функция аутентификации, позволяющая использовать ресурсы на нескольких независимых программных системах в едином процессе аутентификации пользователя. В соответствии с некоторыми вариантами осуществления настоящего изобретения, процедура аутентификации выполняется на основе биологического соответствия и закрытого ключа/открытого ключа, содержащего биометрический код, для сохранения процесса ввода сертификата и пароля, запрашиваемых сервером 130, предоставляющим обслуживание, что позволяет реализовать биометрический единый вход. В соответствии с другими вариантами осуществления настоящего изобретения, пользователь может владеть или располагать коммуникационными терминалами, хранить в собственном облаке пользователя закрытый ключ, сгенерированный первым терминалом (например, смартфоном), и загружать соответствующий закрытый ключ для использования во втором терминале (например, планшетном компьютере, смарт-часах). Это избавляет от необходимости генерировать закрытые ключи с одной и той же целью на соответственных коммуникационных терминалах, и закрытый ключ, генерируемый в одном коммуникационном терминале, может совместно использоваться множеством коммуникационных терминалов, которыми пользователь владеет или располагает.

[00177] Раздел аутентификации пользователя устройства является областью применения для поддержки аутентификации пользователя при регистрации IoT устройства или управлении доступом к IoT устройству. Открытый ключ/закрытый ключ, используемый в такой области применения, вставляют дополнительно с кодом устройства, включая закодированные идентификационные данные IoT устройства, а также биометрический код. Кроме того, открытый ключ передается каждому IoT устройству, централизованному контроллеру, серверу IoT обслуживания, серверу продавца IoT и тому подобному и используется для аутентификации пользователя устройства, дистанционного управления и тому подобного.

[00178] На фиг. 14 приведена схематическая иллюстрация случая, когда различные фрагменты биометрических данных или их комбинация могут быть систематизированы и использованы в различных применениях.

[00179] Как описано выше, в некоторых вариантах осуществления настоящего изобретения может использоваться множество фрагментов различных биометрических данных и/или комбинация фрагментов различных биометрических данных пользователя. Например, фиг. 14 представляет случай использования различных фрагментов биометрических данных одного и того же типа, где 10 фрагментов информации об отпечатках пальцев соответственно используются для различающихся друг от друга видов применения. То есть, в некоторых вариантах осуществления настоящего изобретения фрагменты биометрических данных одного типа соответственно кодируются и вставляются в единый закрытый ключ/открытый ключ, или для каждого фрагмента биометрических данных генерируется отдельный закрытый ключ/открытый ключ.

[00180] Далее, фиг. 14 представляет случай, когда различные комбинации фрагментов биометрических данных используются соответственно для отличающихся друг от друга видов применения. То есть в некоторых вариантах осуществления настоящего изобретения фрагменты биометрических данных кодируются и вставляются соответственно в единый закрытый ключ/открытый ключ, и для каждой из комбинаций может быть сгенерирована отдельная пара ключей (закрытый ключ/открытый ключ). Кроме того, порядок ввода фрагментов биометрических данных может быть приведен к одной и той же комбинации фрагментов биометрических данных.

[00181] В описаниях различных вариантов осуществления настоящего изобретения предполагается, что зашифрованные биометрические данные, используемые для биометрического сопоставления, а также закрытый ключ, в который вставляется биометрический код, хранятся в смарт-карте или коммуникационном терминале во всей общей детализации. Однако не рекомендуется рассматривать такие признаки в качестве обязательных составных элементов во всех вариантах осуществления настоящего изобретения. Например, в некоторых вариантах зашифрованные биометрические данные не хранятся в смарт-карте или коммуникационном терминале, так что для биометрического сопоставления используется только биометрический код, вставленный в закрытый ключ. Дополнительно, в некоторых вариантах осуществления могут быть использованы хэш-значения биометрических данных человека, предоставляемые государственным учреждением (например, администрацией, следственным органом, иммиграционным офисом, и тому подобным). Хэш-значение может быть сохранено заранее, в заданной области смарт-карты, и может быть вставлено в EV домен сертификата открытого ключа, выданного соответствующим органом. Кроме того, зашифрованные биометрические данные, используемые для биометрического сопоставления, могут быть биометрическими данными, которые зашифрованы алгоритмом шифрования, определенным в сертификате открытого ключа, и могут быть биометрическими данными, зашифрованными с помощью закрытого ключа, в который вставляется биометрический код. Кроме того, биометрические данные, зашифрованные с помощью сертификата открытого ключа, могут быть сохранены с закрытым ключом в состоянии, в котором зашифрованные биометрические данные дополнительно зашифрованы с закрытым ключом.

[00182] Вышеупомянутые способы в соответствии с некоторыми вариантами осуществления настоящего изобретения могут также быть реализованы в качестве машиночитаемого кода на машиночитаемом записывающем носителе. Машиночитаемый записывающий носитель - это любое устройство хранения данных, которое может хранить данные, которые впоследствии могут быть считаны компьютерной системой. Примеры машиночитаемого записывающего носителя включают в себя магнитные запоминающие носители (например, ROM, гибкие диски, жесткие диски и так далее), оптические записывающие носители (например, компакт-диски или DVD-диски) и так далее, и несущие волны (например, передачи по сети Интернет). Машиночитаемый записывающий носитель также может быть распределен по связанным по сети компьютерным системам, так что машиночитаемый код сохраняется и исполняется распределенным образом.

[00183] Хотя примерные варианты осуществления настоящего изобретения были описаны для иллюстративных целей, специалистам в данной области техники очевидно, что различные модификации, добавления и замены возможны без отхода от идеи и объема заявленного изобретения. Конкретные термины, используемые в настоящем описании и чертежах, используются в иллюстративных целях и не должны рассматриваться в качестве ограничений настоящего изобретения. Таким образом, примерные варианты осуществления настоящего изобретения были описаны для краткости и ясности. Соответственно, специалисту в данной области техники очевидно, что объем правовой охраны заявленного изобретения не ограничен явно описанными выше вариантами осуществления и определяется формулой изобретения и ее эквивалентами.

## (57) Формула изобретения

1. Способ регистрации человека в качестве авторизованного пользователя IoT (Интернет вещей) устройства, при этом способ содержит:

- сбор посредством портативного устройства биометрических данных или комбинации фрагментов биометрических данных человека;

- генерацию биометрического кода из биометрических данных или комбинации фрагментов биометрических данных человека;

- сбор уникальных идентификационных данных IoT устройства;

- генерацию кода IoT устройства из уникальных идентификационных данных IoT устройства;

- вставку в поле расширения сертификата открытого ключа, хранящегося в портативном устройстве, проверочного кода, содержащего биометрический код и код IoT устройства;

- генерацию пары, содержащей закрытый ключ и открытый ключ, причем закрытый ключ содержит проверочный код; и

- передачу открытого ключа на удаленный объект, связанный с IoT устройством, с обеспечением тем самым возможности регистрации человека удаленным объектом в качестве авторизованного пользователя IoT устройства.

2. Способ по п.1, в котором проверочный код дополнительно содержит код, сгенерированный из уникальных идентификационных данных, закрепленных за портативным устройством, код, сгенерированный из характеристической информации, указывающей характеристики поведения человека, код, сгенерированный из информации о местоположении, указывающей на позицию, в которую предполагается отправить информацию об аутентификации, код, сгенерированный из уникальных идентификационных данных, закрепленных за человеком, или их комбинацию.

3. Способ по п.1, дополнительно содержащий хранение биометрических данных или комбинации фрагментов биометрических данных человека в портативном устройстве.

4. Способ по п.3, дополнительно содержащий шифрование, перед хранением, биометрических данных или комбинации фрагментов биометрических данных.

5. Способ по п.1, дополнительно содержащий хранение закрытого ключа в портативном устройстве.

6. Способ по п.1, дополнительно содержащий:

- сбор добавочных биометрических данных или добавочной комбинации фрагментов биометрических данных человека, отличающихся от биометрических данных или комбинации фрагментов биометрических данных человека согласно п.1;

- генерирование добавочного биометрического кода из добавочных биометрических данных или добавочной комбинации фрагментов биометрических данных человека; и

- вставку, в поле расширения сертификата открытого ключа, добавочного проверочного кода, содержащего добавочный биометрический код; причем закрытый ключ содержит добавочный проверочный код.

7. Способ по п.6, в котором добавочный проверочный код и проверочный код согласно п. 1 имеют отличающиеся применения.

8. Способ по п.7, в котором добавочный проверочный код предназначен для (a) уведомления о ситуации, в которой закрытый ключ используется принудительно, (b) запроса удаленного объекта на отмену регистрации, (c) запроса удаленного объекта на возврат процесса регистрации в заданное предыдущее состояние, или (d) запроса удаленного объекта на инициализацию системы управления аутентификацией, которая может управляться удаленным объектом.

9. Способ по п.1, в котором поле расширения сертификата открытого ключа

дополнительно содержит информацию об электронной карте резидента человека, водительских правах человека, электронных деньгах человека, или медицинской карте человека, URL (унифицированном указателе ресурсов) удаленного объекта, или их комбинации.

10. Способ по п.1, дополнительно содержащий:

- сбор добавочных биометрических данных или добавочной комбинации фрагментов биометрических данных человека, отличающихся от биометрических данных или комбинации фрагментов биометрических данных человека согласно п.1;

- генерацию добавочного биометрического кода из добавочных биометрических данных или добавочной комбинации фрагментов биометрических данных человека;

- вставку в поле расширения добавочного сертификата открытого ключа, хранящегося в портативном устройстве, добавочного проверочного кода, содержащего добавочный биометрический код и код IoT устройства; и

- генерацию добавочной пары, содержащей закрытый ключ и открытый ключ, причем закрытый ключ содержит добавочный проверочный код.

11. Способ по п.1, дополнительно содержащий:

- сбор добавочных биометрических данных или добавочной комбинации фрагментов биометрических данных человека, отличающихся от биометрических данных или комбинации фрагментов биометрических данных человека согласно п. 1;

- генерацию добавочного биометрического кода из добавочных биометрических данных или добавочной комбинации фрагментов биометрических данных;

- сбор уникальных идентификационных данных дополнительного IoT устройства;

- генерацию добавочного кода IoT устройства из уникальных идентификационных данных добавочного IoT устройства;

- вставку в поле расширения добавочного сертификата открытого ключа, хранящегося в портативном устройстве, добавочного проверочного кода, содержащего добавочный биометрический код и добавочный код IoT устройства; и

- генерацию добавочной пары, содержащей закрытый ключ и открытый ключ, причем закрытый ключ добавочной пары содержит добавочный проверочный код.

12. Способ по п.1, в котором открытый ключ передают на удаленный объект через виртуальную частную сеть.

13. Способ по п.1, в котором портативное устройство выполнено в виде смарт-карты, шифратора или мобильного коммуникационного терминала.

14. Способ содействия, с помощью портативного устройства, определению посредством удаленного объекта того, является ли человек, который запрашивает у портативного устройства доступ к IoT устройству, тем же человеком, который зарегистрирован в качестве авторизованного пользователя IoT устройства, при этом портативное устройство хранит биометрические данные или комбинацию фрагментов биометрических данных человека, который зарегистрирован в качестве авторизованного пользователя IoT устройства, и портативное устройство хранит закрытый ключ, содержащий проверочный код, включающий в себя (1) биометрический код, сгенерированный из биометрических данных или комбинации фрагментов биометрических данных человека, который зарегистрирован в качестве авторизованного пользователя IoT устройства, и (2) код IoT устройства, сгенерированный из уникальных идентификационных данных IoT устройства, при этом способ содержит:

- сбор биометрических данных или комбинации фрагментов биометрических данных человека, который запрашивает у портативного устройства доступ к IoT устройству;

- определение того, совпадают ли собранные биометрические данные или собранная

комбинация фрагментов биометрических данных человека, который запрашивает у портативного устройства доступ к IoT устройству, с хранящимися биометрическими данными или с хранящейся комбинацией фрагментов биометрических данных человека, который зарегистрирован в качестве авторизованного пользователя IoT устройства;

- создание информации об аутентификации, содержащей проверочный код, когда определено их соответствие; и

- передачу удаленному объекту информации об аутентификации, с обеспечением тем самым возможности определения посредством удаленного объекта того, является ли человек, который запрашивает у портативного устройства доступ к IoT устройству, тем же человеком, который зарегистрирован в качестве авторизованного пользователя IoT устройства.

15. Способ по п. 14, дополнительно содержащий:

- определение того, совпадают ли собранные биометрические данные или собранная комбинация фрагментов биометрических данных человека, который запрашивает у портативного устройства доступ к IoT устройству, с биометрическим кодом, содержащимся в закрытом ключе; и

- создание информации об аутентификации, когда определено, что собранные биометрические данные или собранная комбинация фрагментов биометрических данных человека, который запрашивает у портативного устройства доступ к IoT устройству, совпадает как с (a) хранящимися биометрическими данными или хранящейся комбинацией фрагментов биометрических данных человека, зарегистрированного в качестве авторизованного пользователя IoT устройства, так и с (b) биометрическим кодом, хранящимся в закрытом ключе.

16. Способ по п.14, в котором проверочный код дополнительно содержит код, сгенерированный из уникальных идентификационных данных, закрепленных за портативным устройством, код, сгенерированный из информации о местоположении, указывающей позицию, в которую предполагается отправить информацию об аутентификации, код, сгенерированный из уникальных идентификационных данных, закрепленных за человеком, который зарегистрирован в качестве авторизованного пользователя IoT устройства, код, сгенерированный из характеристической информации, указывающей характеристики поведения человека, который зарегистрирован в качестве авторизованного пользователя IoT устройства, или их комбинацию.

17. Способ по п.14, в котором информация об аутентификации дополнительно включает в себя (a) информацию, соответствующую OTP (одноразовый пароль), (b) информацию о времени передачи информации об аутентификации, (c) информацию о времени генерации закрытого ключа, (d) информацию о местоположении позиции, из которой отправлена информация об аутентификации, или (e) их комбинацию.

18. Способ по п.14, в котором информацию об аутентификации передают на удаленный объект через виртуальную частную сеть.

19. Способ по п.18, в котором URL (унифицированный указатель ресурса) назначения в виртуальной частной сети содержится в закрытом ключе.

20. Способ по п.14, в котором портативное устройство выполнено в виде смарт-карты, шифратора или мобильного коммуникационного терминала.

21. Способ по п. 14, в котором удаленный объект представляет собой сервер, коммуникационный терминал, IoT устройство или другое IoT устройство, связанное с IoT устройством.

22. Способ подтверждения, посредством удаленного объекта, того, является ли человек, который запрашивает у портативного устройства доступ к IoT устройству,

тем же человеком, который зарегистрирован в качестве авторизованного пользователя IoT устройства, причем портативное устройство включает в себя пару, содержащую открытый ключ и закрытый ключ, и закрытый ключ содержит проверочный код, включающий в себя (1) биометрический код, сгенерированный из биометрических данных или комбинации фрагментов биометрических данных авторизованного пользователя IoT устройства, и (2) код IoT устройства, сгенерированный из уникальных идентификационных данных IoT устройства, при этом способ содержит:

- получение открытого ключа от портативного устройства, с обеспечением тем самым регистрации человека, желающего зарегистрироваться в качестве авторизованного пользователя IoT устройства;

- получение от портативного устройства информации об аутентификации, содержащей проверочный код, причем информацию об аутентификации создают в портативном устройстве, когда в портативном устройстве определено, что биометрические данные или комбинации фрагментов биометрических данных человека, который запрашивает у портативного устройства доступ к IoT устройству, совпадают с биометрическими данными или с комбинацией фрагментов биометрических данных авторизованного пользователя IoT устройства;

- проверку информации об аутентификации путем использования открытого ключа; и

- подтверждение того, является ли человек, который запрашивает у портативного устройства доступ к IoT устройству, тем же человеком, который является авторизованным пользователем IoT устройства, по результатам проверки.

23. Способ по п. 22, в котором информацию об идентификации создают, когда дополнительно определено, что биометрические данные или комбинация фрагментов биометрических данных человека, который запрашивает у портативного устройства доступ к IoT устройству, совпадают с биометрическими данными, содержащимися в закрытом ключе.

24. Способ по п. 22, в котором удаленный объект представляет собой сервер, коммуникационный терминал, IoT устройство или другое IoT устройство, связанное с IoT устройством.

25. Способ аутентификации пользователя обслуживанием в системе управления аутентификацией на основе сертификата открытого ключа, при этом способ содержит:

- получение на сервере, предоставляющем обслуживание и выполненном с возможностью управления открытым терминалом, выполненным с возможностью предоставления заданного обслуживания, открытого ключа от портативного устройства человека, причем открытый ключ соответствует закрытому ключу, содержащему проверочный код, включающий в себя биометрический код, полученный из биометрических данных или комбинации фрагментов биометрических данных человека;

- регистрацию на сервере, предоставляющем обслуживание, путем использования открытого ключа, человека в качестве авторизованного пользователя заданного обслуживания;

- получение на открытом терминале информации об аутентификации от портативного устройства, причем информация об аутентификации содержит проверочный код;

- запрос, на открытом терминале, сервера, предоставляющего обслуживание, о проверке на основе открытого ключа информации об аутентификации;

- аутентификацию сервером, предоставляющим обслуживание, пользователя обслуживанием на основе результатов проверки; и

- предоставление открытым терминалом предусмотренного обслуживания при его

аутентификации.

26. Способ по п.25, дополнительно содержащий:

- изменение сервером, предоставляющим обслуживание, открытого ключа для генерации модифицированного открытого ключа, который включает в себя проверочный код, причем модифицированный открытый ключ сконфигурирован для использования, когда сервер, предоставляющий обслуживание, недоступен; и

- передачу сервером, предоставляющим обслуживание, модифицированного открытого ключа к портативному устройству.

27. Способ по п.26, дополнительно содержащий:

- получение открытым терминалом проверочного кода закрытого ключа и проверочного кода модифицированного открытого ключа от портативного устройства, когда сервер, предоставляющий обслуживание, недоступен;

- определение открытым терминалом, генерируются ли оба проверочных кода на основе одного и того же сертификата открытого ключа; и

- предоставление открытым терминалом по меньшей мере некоторых вариантов из заданного обслуживания, когда определено, что оба проверочных кода генерируются на основе одного и того же сертификата открытого ключа.

28. Способ по п. 27, дополнительно содержащий:

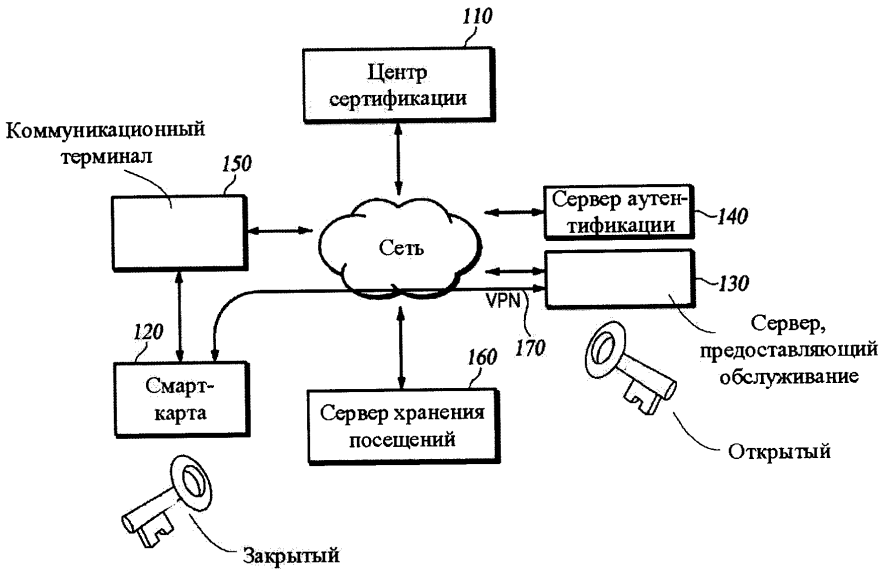
- передачу открытым терминалом обоих проверочных кодов и информации о предоставленном обслуживании серверу, предоставляющему обслуживание, когда сервер, предоставляющий обслуживание, становится доступным;

- проверку сервером, предоставляющим обслуживание, проверочных кодов; и

- обновление сервером, предоставляющим обслуживание, записей сервера, предоставляющего обслуживание, когда проверочные коды проверены.

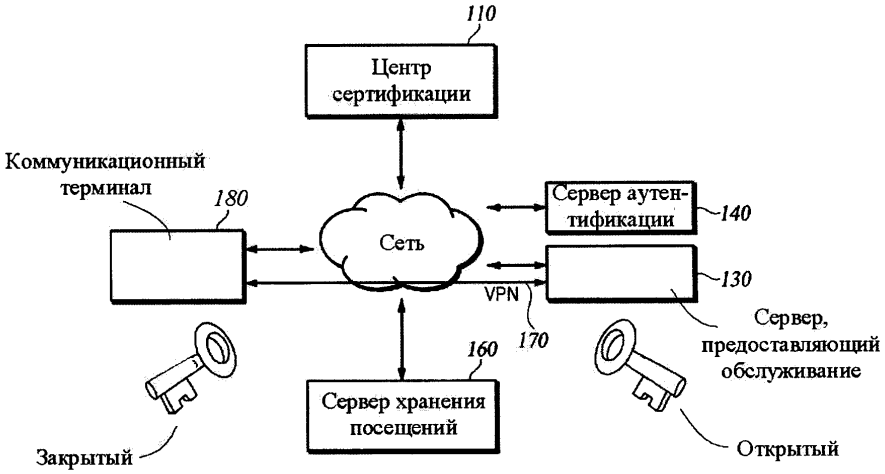
1




110
Центр сертификации
Коммуникационный терминал
150
Сеть
Сервер аутен-тификации
140
130
VPN
170
120
160
Смарт-карта
Сервер хранения посещений
Сервер, предоставляющий обслуживание
Открытый
Закрытый

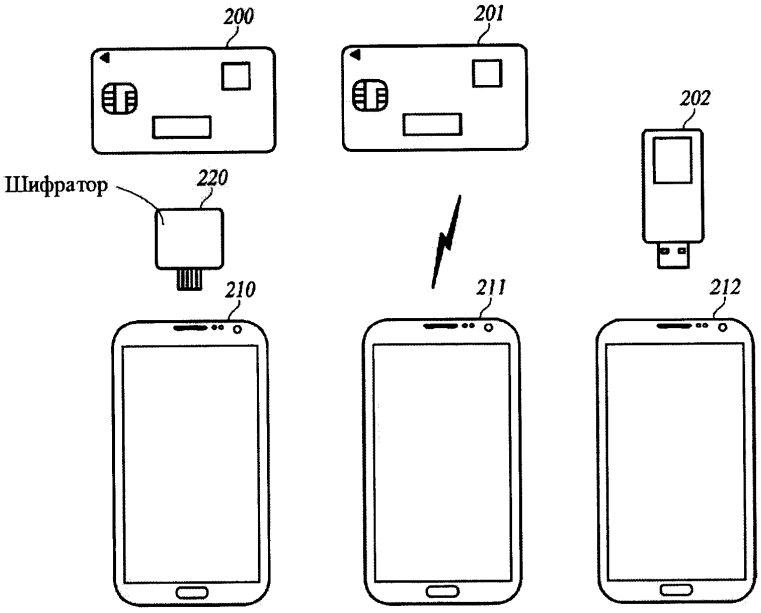
Фиг. 1A

2


110
Центр сертификации
Коммуникационный терминал
180
Сеть
Сервер аутен-тификации
140
130
VPN
170
Сервер, предоставляющий обслуживание
160
Сервер хранения посещений
Закрытый
Открытый

Фиг. 1B

3



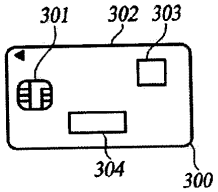

Фиг. 2A Фиг. 2B Фиг. 2C

4

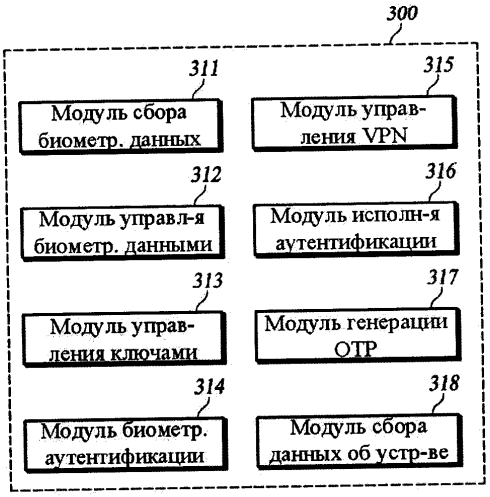
| Функциональный состав |
| --- |
| • Модуль сбора биометрических данных<br>• Модуль управления биометр. данными<br>• Модуль биометр. аутентификации<br>• Модуль сбора данных об устройстве<br>• Модуль управления VPN<br>• Модуль генерации OTP<br>• Модуль управления ключами<br>• Модуль исполнения аутентификации |

| Физический состав |
| --- |
| • Блок центр. процессора (CPU)<br>• Память<br>• Порт входа/выхода<br>• Дисплей (опция)<br>• Биометрический датчик (опция)<br>• Схема физически неклонируемой функций (PUF) (опция) |

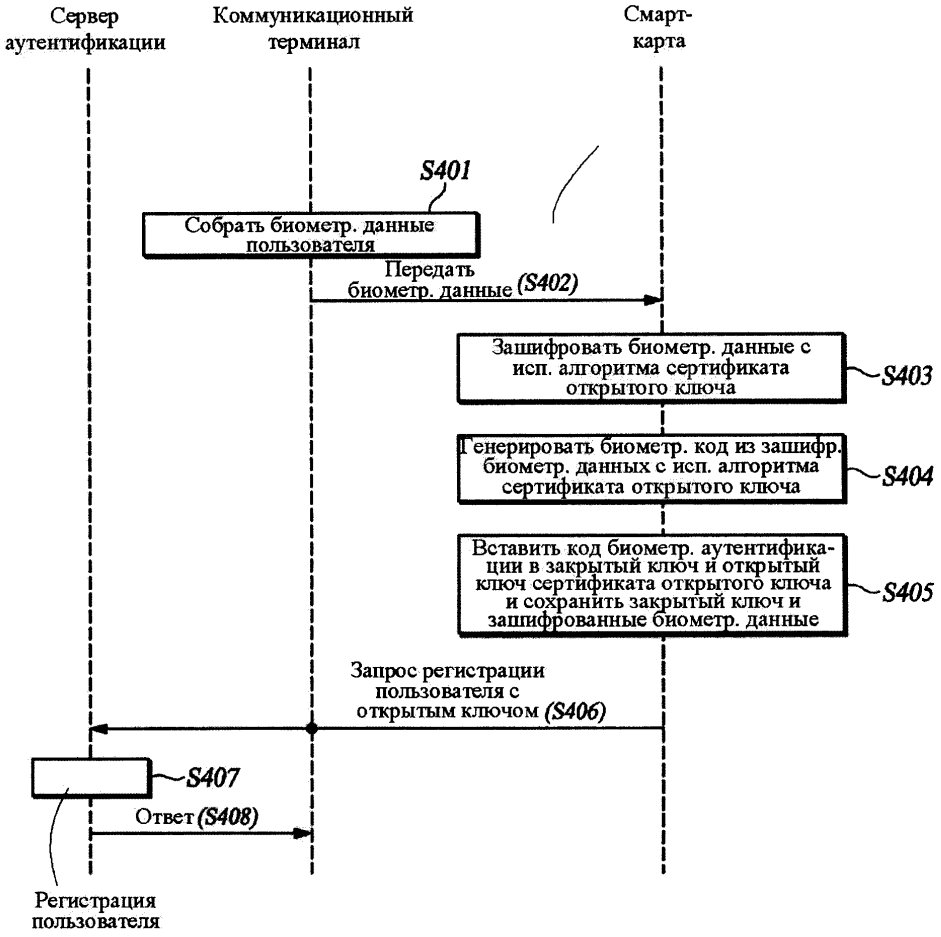
Фиг. 3A




Фиг. 3B

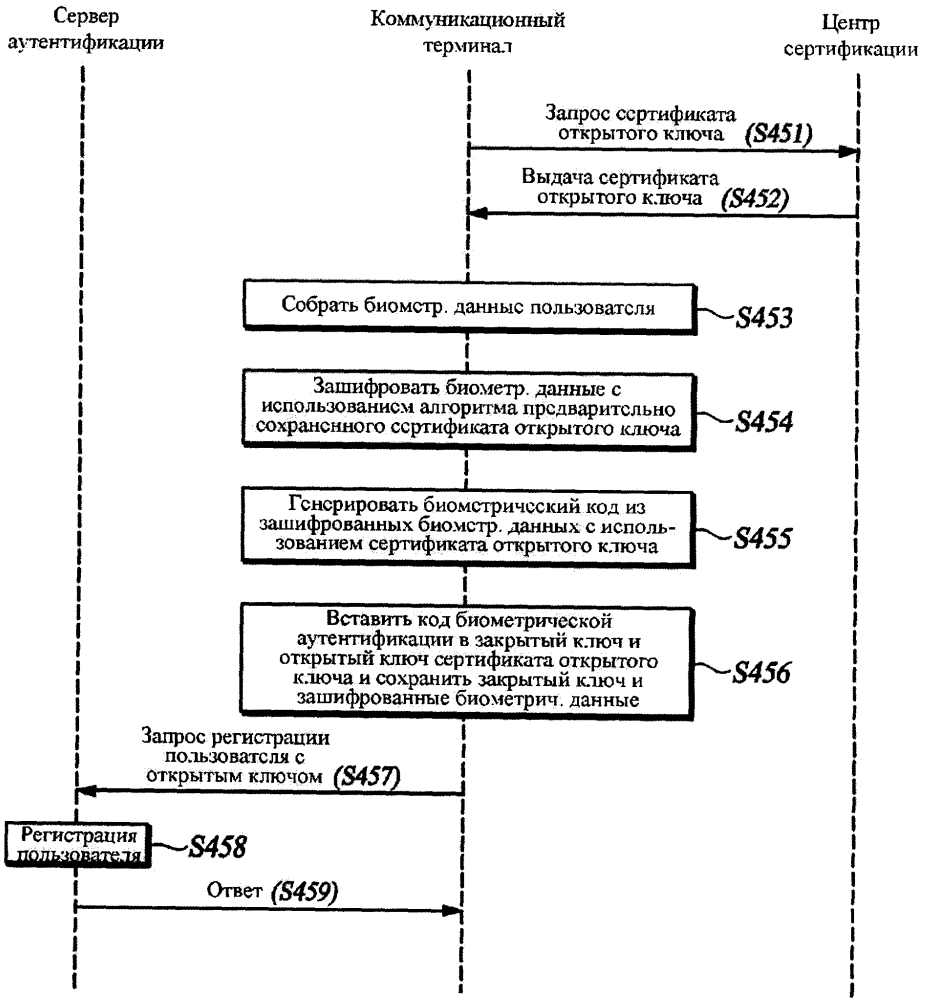



Фиг. 3C


Сервер аутентификации
Коммуникационный терминал
Смарт-карта
S401
Собрать биометр. данные пользователя
Передать биометр. данные (S402)
Зашифровать биометр. данные с исп. алгоритма сертификата открытого ключа
S403
Генерировать биометр. код из зашифр. биометр. данных с исп. алгоритма сертификата открытого ключа
S404
Вставить код биометр. аутентификации в закрытый ключ и открытый ключ сертификата открытого ключа и сохранить закрытый ключ и зашифрованные биометр. данные
S405
Запрос регистрации пользователя с открытым ключом (S406)
S407
Ответ (S408)
Регистрация пользователя

Фиг. 4A

6


Сервер аутентификации
Коммуникационный терминал
Центр сертификации
Запрос сертификата открытого ключа (S451)
Выдача сертификата открытого ключа (S452)
Собрать биометр. данные пользователя
S453
Зашифровать биометр. данные с использованием алгоритма предварительно сохраненного сертификата открытого ключа
S454
Генерировать биометрический код из зашифрованных биометр. данных с использованием сертификата открытого ключа
S455
Вставить код биометрической аутентификации в закрытый ключ и открытый ключ сертификата открытого ключа и сохранить закрытый ключ и зашифрованные биометрич. данные
S456
Запрос регистрации пользователя с открытым ключом (S457)
Регистрация пользователя
S458
Ответ (S459)

Фиг. 4B

7

<Перед регистрацией пользователя>

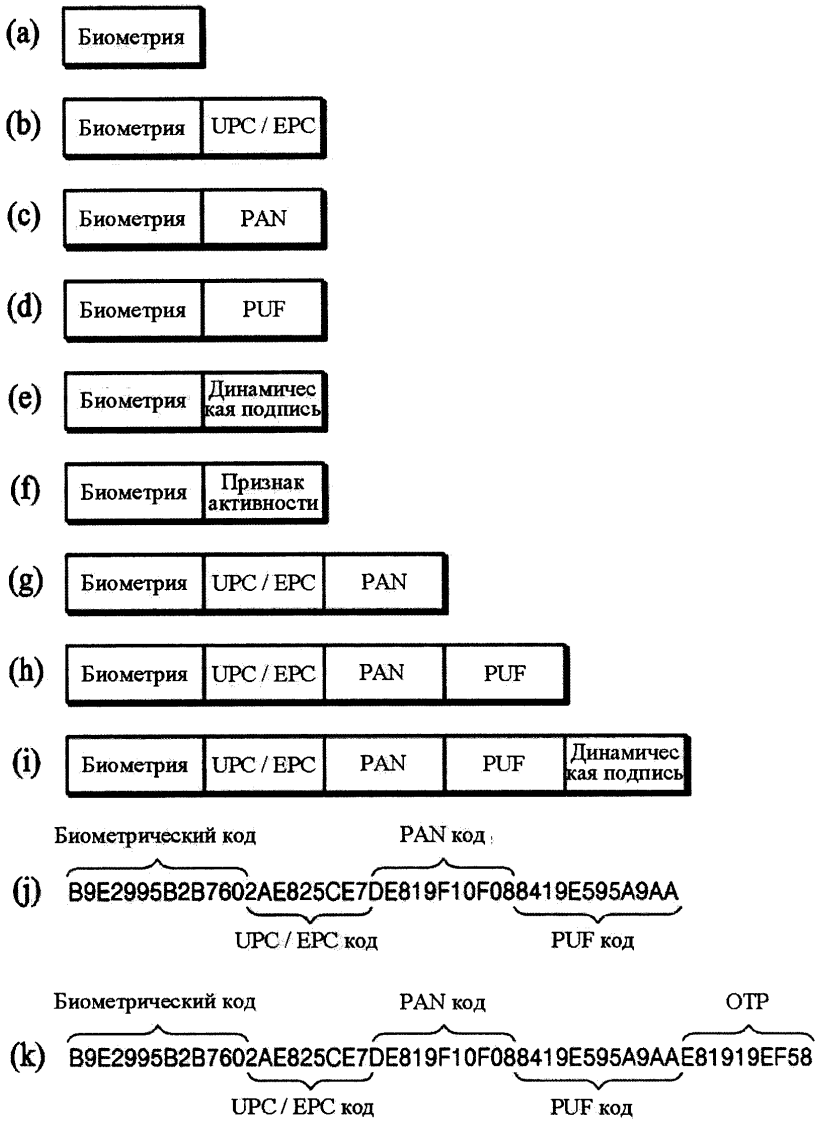
| Сертификат открытого ключа |
| --- |
| Версия / Серийный номер / Алгоритм подписи / Хэш-алгоритм / Наименование выпускающего органа / Срок действия / Открытый ключ<br>Отличительное имя субъекта / Информация об открытом ключе субъекта / Подпись выпускающего органа |
| Расширенная проверка |
| (Пустой) |

Фиг. 5A

<После регистрации пользователя>

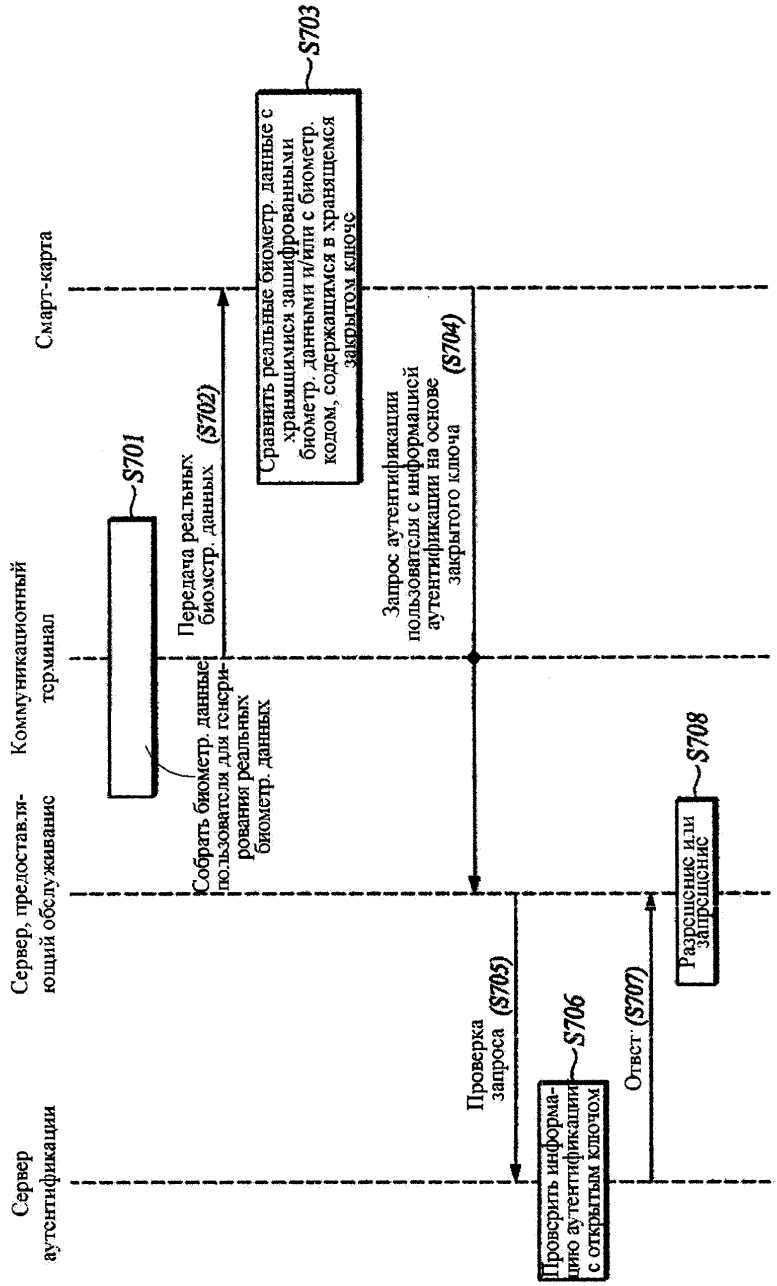
| Сертификат открытого ключа |
| --- |
| Версия / Серийный номер / Алгоритм подписи / Хэш-алгоритм / Наименование выпускающего органа / Срок действия / Открытый ключ<br>Отличительное имя субъекта / Информация об открытом ключе субъекта / Подпись выпускающего органа |
| Расширенная проверка |
| • Биометрический код + под меньшей мере один добавочный код<br>  Штрих-код/QR/UPC/RFID/URL/ CRL/PUF/GSI/GSIN/IPv6/MAC/ Адрес криптогра-фических хэш-функций/уникальная идентифика-ционная информация и т.д. |

Фиг. 5B

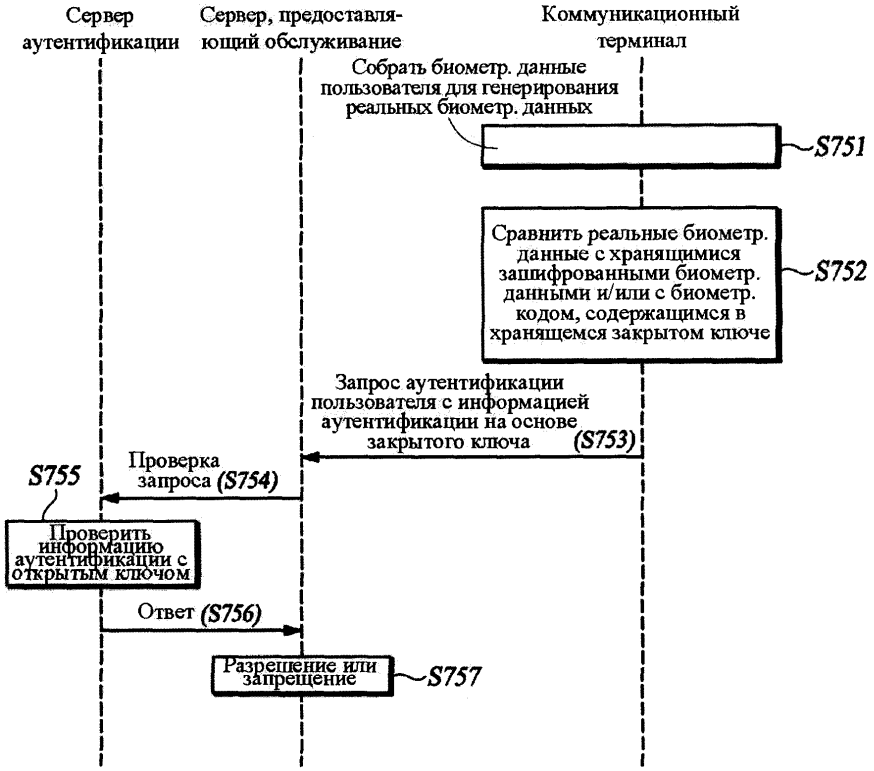

(a)
Биометрия
(b)
Биометрия
UPC / EPC
(c)
Биометрия
PAN
(d)
Биометрия
PUF
(e)
Биометрия
Динамическая подпись
(f)
Биометрия
Признак активности
(g)
Биометрия
UPC / EPC
PAN
(h)
Биометрия
UPC / EPC
PAN
PUF
(i)
Биометрия
UPC / EPC
PAN
PUF
Динамическая подпись
Биометрический код
PAN код
(j)
B9E2995B2B7602AE825CE7DE819F10F088419E595A9AA
UPC / EPC код
PUF код
Биометрический код
PAN код
OTP
(k)
B9E2995B2B7602AE825CE7DE819F10F088419E595A9AAE81919EF58
UPC / EPC код
PUF код

Фиг. 6

9


Сервер аутентификации
Сервер, предоставляющий обслуживание
Коммуникационный терминал
Смарт-карта
S701
Собрать биометр. данные пользователя для генерирования реальных биометр. данных
Передача реальных биометр. данных (S702)
S703
Сравнить реальные биометр. данные с хранящимися зашифрованными биометр. данными и/или с биометр. кодом, содержащимся в хранящемся закрытом ключе
Запрос аутентификации пользователя с информацией аутентификации на основе закрытого ключа (S704)
Проверка запроса (S705)
S706
Проверить информацию аутентификации с открытым ключом
Ответ (S707)
S708
Разрешение или запрещение

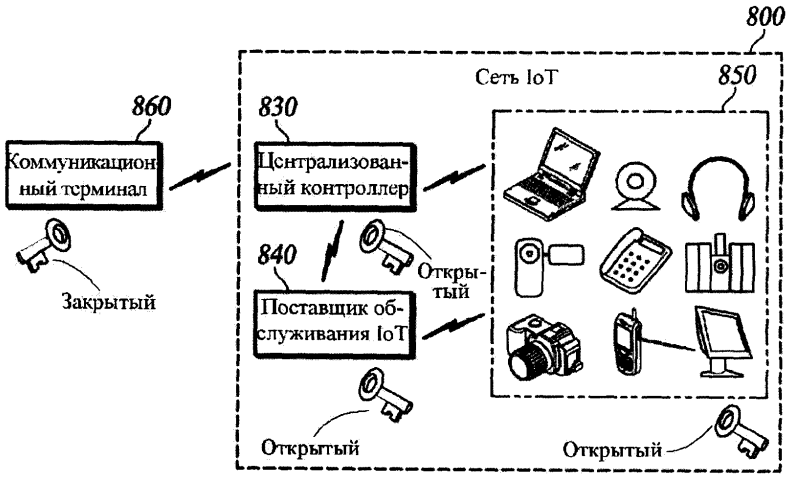
Фиг. 7А


Сервер аутентификации
Сервер, предоставляющий обслуживание
Коммуникационный терминал
Собрать биометр. данные пользователя для генерирования реальных биометр. данных
S751
Сравнить реальные биометр. данные с хранящимися зашифрованными биометр. данными и/или с биометр. кодом, содержащимся в хранящемся закрытом ключе
S752
Запрос аутентификации пользователя с информацией аутентификации на основе закрытого ключа (S753)
S755
Проверка запроса (S754)
Проверить информацию аутентификации с открытым ключом
Ответ (S756)
Разрешение или запрещение
S757

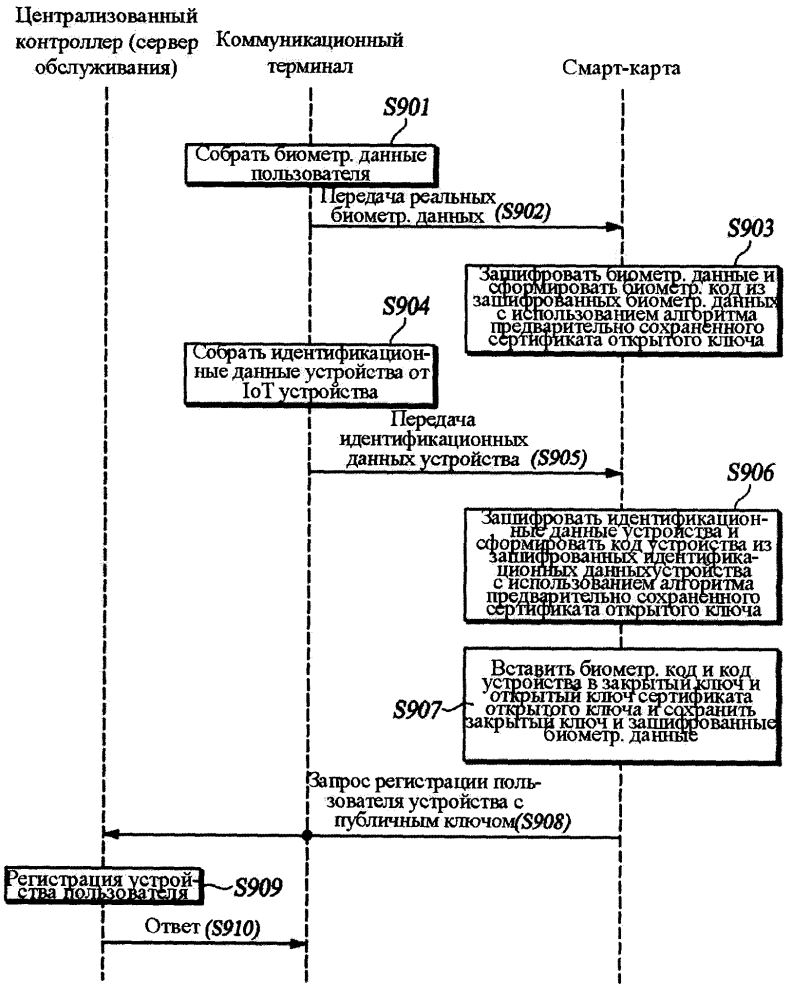
Фиг. 7B


800
820
Сеть IoT
850
Коммуникационный терминал
810
830
Открытый
Смарт-карта
Централизованный контроллер
840
Закрытый
Открытый
Поставщик обслуживания IoT
Открытый
Открытый

Фиг. 8A

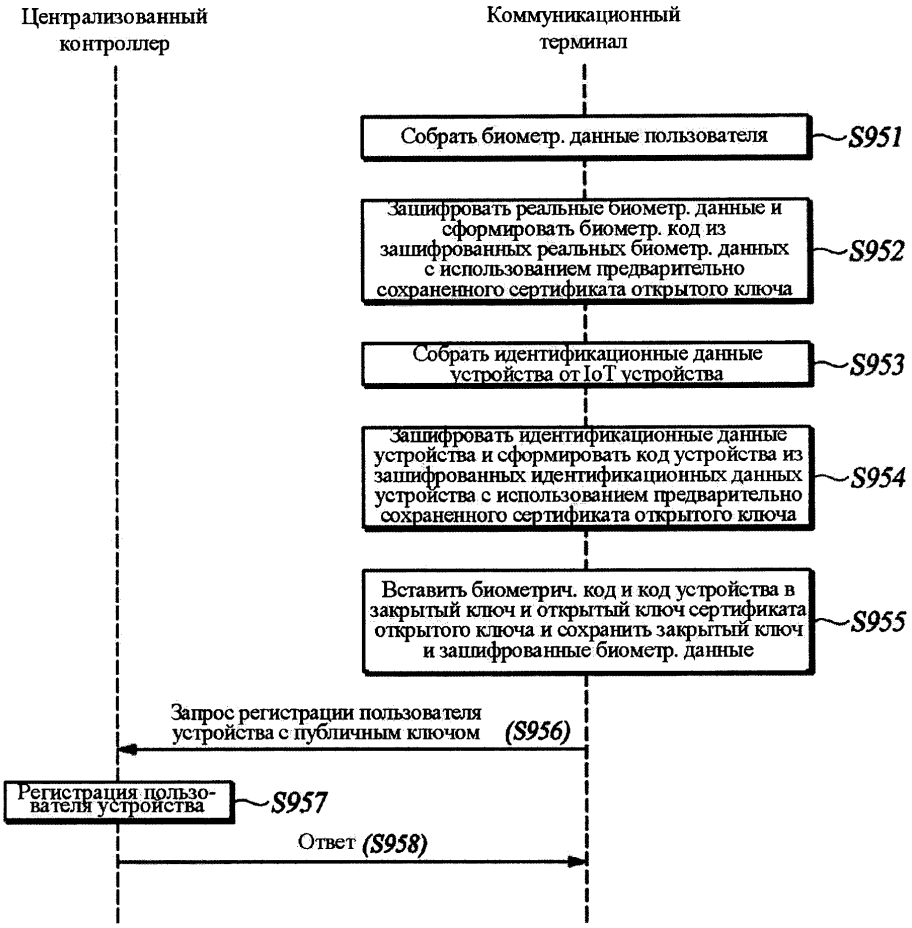

800
Сеть IoT
850
860
830
Коммуникационный терминал
Централизованный контроллер
840
Открытый
Поставщик обслуживания IoT
Закрытый
Открытый
Открытый

Фиг. 8B


Централизованный контроллер (сервер обслуживания)
Коммуникационный терминал
Смарт-карта
S901
Собрать биометр. данные пользователя
Передача реальных биометр. данных (S902)
S903
Зашифровать биометр. данные и сформировать биометр. код из зашифрованных биометр. данных с использованием алгоритма предварительно сохраненного сертификата открытого ключа
S904
Собрать идентификационные данные устройства от IoT устройства
Передача идентификационных данных устройства (S905)
S906
Зашифровать идентификационные данные устройства и сформировать код устройства из зашифрованных идентификационных данныхустройства с использованием алгоритма предварительно сохраненного сертификата открытого ключа
Вставить биометр. код и код устройства в закрытый ключ и открытый ключ сертификата открытого ключа и сохранить закрытый ключ и зашифрованные биометр. данные
S907
Запрос регистрации пользователя устройства с публичным ключом(S908)
Регистрация устройства пользователя
S909
Ответ (S910)

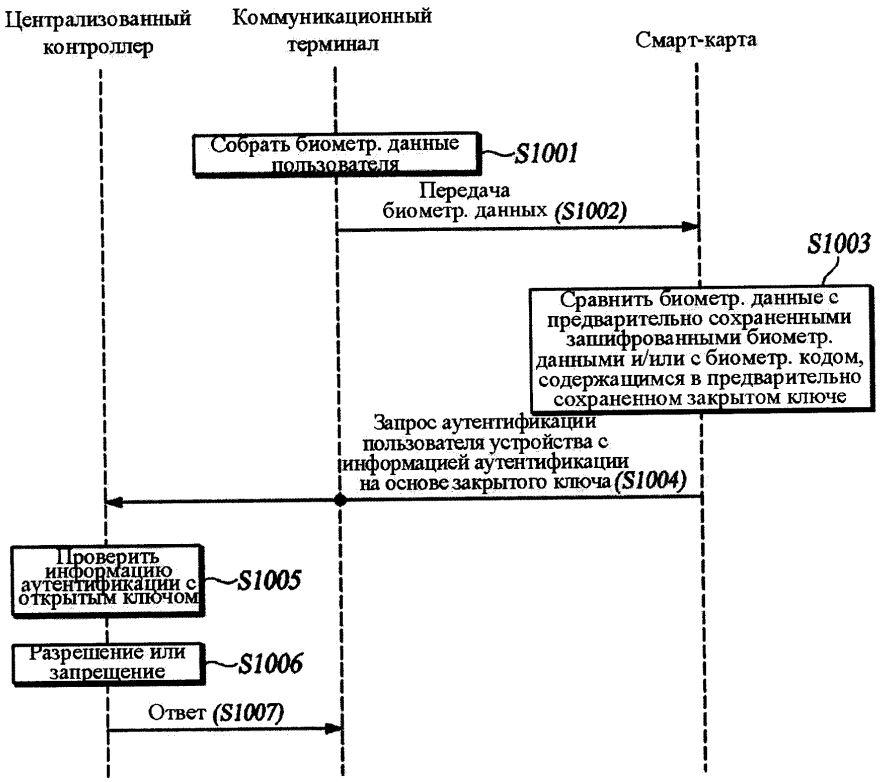
Фиг. 9A

14


Централизованный контроллер
Коммуникационный терминал
Собрать биометр. данные пользователя
S951
Зашифровать реальные биометр. данные и сформировать биометр. код из зашифрованных реальных биометр. данных с использованием предварительно сохраненного сертификата открытого ключа
S952
Собрать идентификационные данные устройства от IoT устройства
S953
Зашифровать идентификационные данные устройства и сформировать код устройства из зашифрованных идентификационных данных устройства с использованием предварительно сохраненного сертификата открытого ключа
S954
Вставить биометрич. код и код устройства в закрытый ключ и открытый ключ сертификата открытого ключа и сохранить закрытый ключ и зашифрованные биометр. данные
S955
Запрос регистрации пользователя устройства с публичным ключом (S956)
Регистрация пользователя устройства
S957
Ответ (S958)

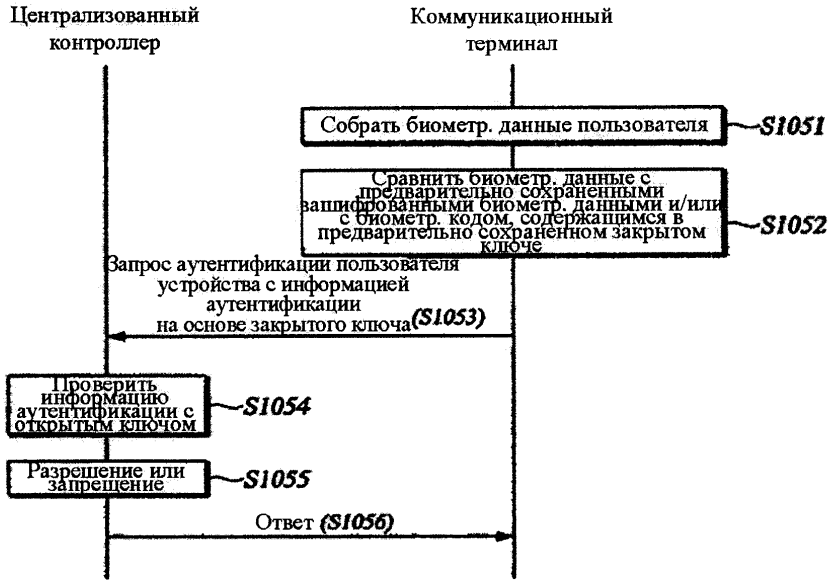
Фиг. 9B

15

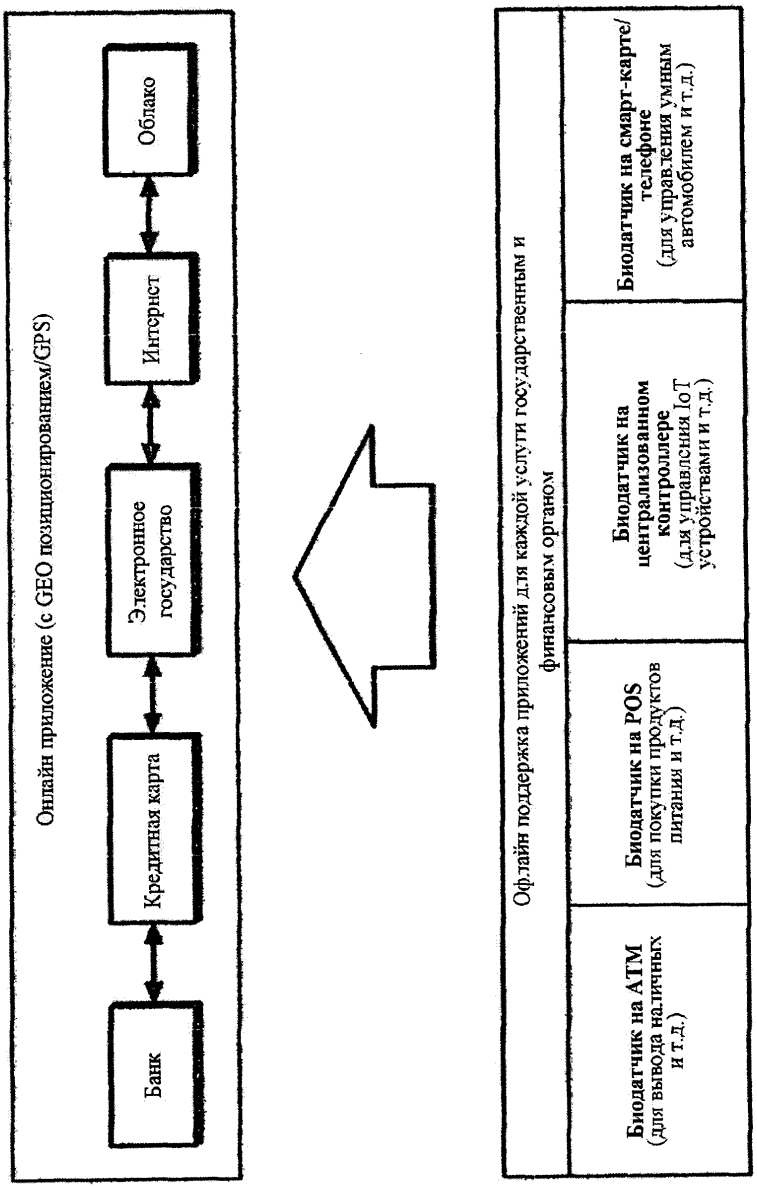

Централизованный контроллер
Коммуникационный терминал
Смарт-карта
Собрать биометр. данные пользователя
S1001
Передача биометр. данных (S1002)
S1003
Сравнить биометр. данные с предварительно сохраненными зашифрованными биометр. данными и/или с биометр. кодом, содержащимся в предварительно сохраненном закрытом ключе
Запрос аутентификации пользователя устройства с информацией аутентификации на основе закрытого ключа (S1004)
Проверить информацию аутентификации с открытым ключом
S1005
Разрешение или запрещение
S1006
Ответ (S1007)

Фиг. 10A

16

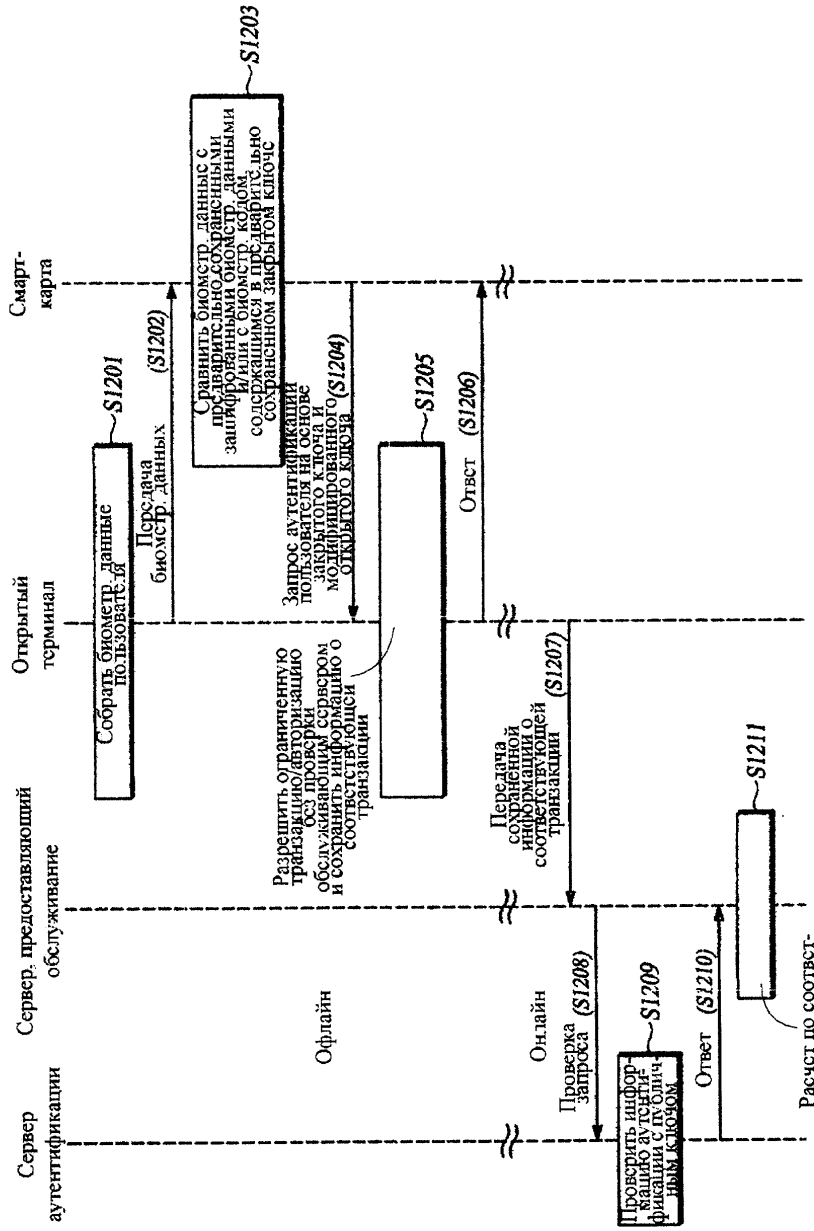

Централизованный контроллер
Коммуникационный терминал
Собрать биометр. данные пользователя
S1051
Сравнить биометр. данные с предварительно сохраненными зашифрованными биометр. данными и/или с биометр. кодом, содержащимся в предварительно сохраненном закрытом ключе
S1052
Запрос аутентификации пользователя устройства с информацией аутентификации на основе закрытого ключа (S1053)
Проверить информацию аутентификации с открытым ключом
S1054
Разрешение или запрещение
S1055
Ответ (S1056)

Фиг. 10B


Онлайн приложение (с GEO позиционированием/GPS)
Банк
Кредитная карта
Электронное государство
Интернет
Облако
Офлайн поддержка приложений для каждой услуги государственным и финансовым органом
Биодатчик на ATM (для вывода наличных и т.д.)
Биодатчик на POS (для покупки продуктов питания и т.д.)
Биодатчик на централизованном контроллере (для управления IoT устройствами и т.д.)
Биодатчик на смарт-карте/телефоне (для управления умным автомобилем и т.д.)

Фиг. 11

18


Смарт-карта
Открытый терминал
Сервер, предоставляющий обслуживание
Сервер аутентификации
Собрать биометр. данные пользователя
S1201
Передача биометр. данных
(S1202)
Сравнить биометр. данные с предварительно сохраненными зашифрованными биометр. данными и/или с биометр. ключом, содержащимся в предварительно сохраненном закрытом ключе
S1203
Запрос аутентификации пользователя на основе закрытого ключа и модифицированного открытого ключа
(S1204)
S1205
Ответ
(S1206)
Разрешить ограничение транзакцию/авторизацию обслуживающим сервером без проверки и сохранить информацию о соответствующей транзакции
Передача сохраненной информации о соответствующей транзакции
(S1207)
Офлайн
Онлайн
Проверка запроса
(S1208)
Проверить информацию аутентификации с публичным ключом
S1209
Ответ
(S1210)
S1211
Расчет по соответствующей транзакции

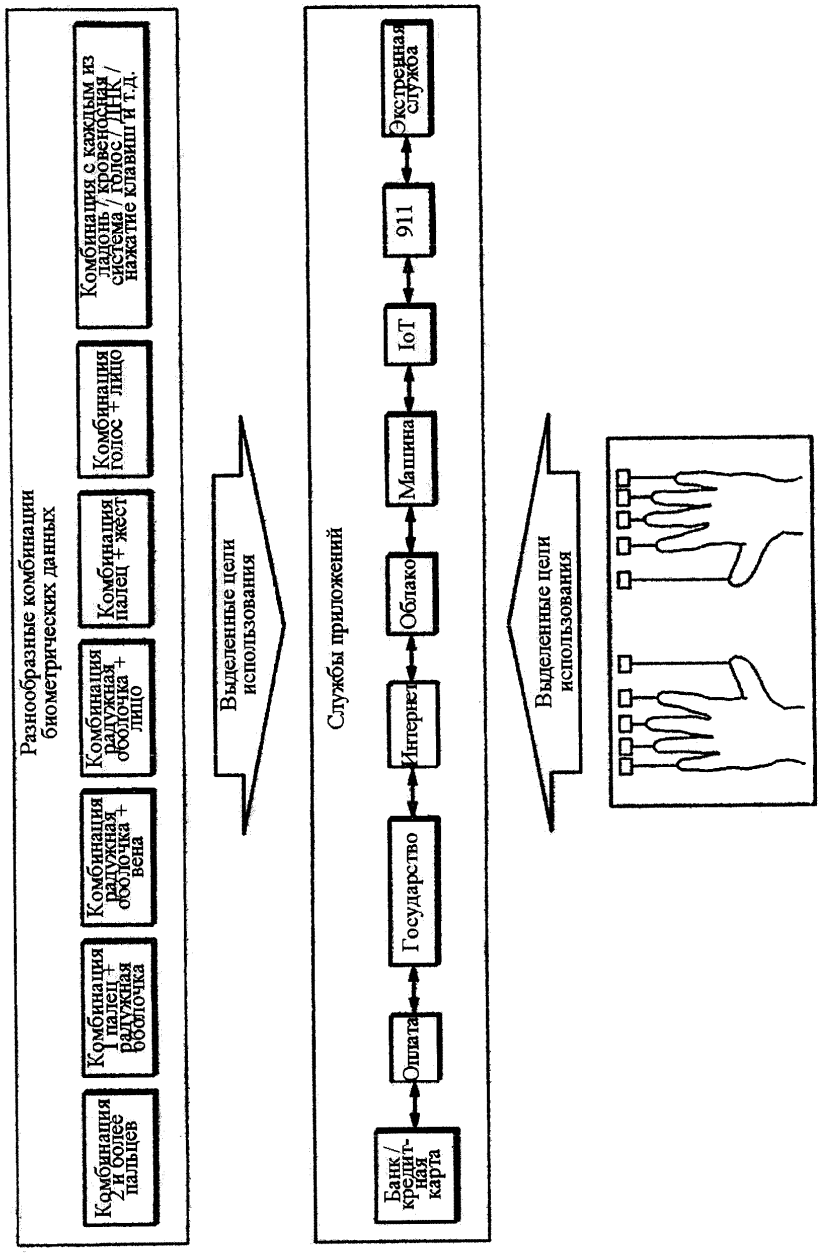
Фиг. 12

19

| Сфера приложений | | | |
|---|---|---|---|
| Финансовый и идентификационный раздел | Физический раздел | Раздел SSO (технологии единого входа) | Раздел аутентификации пользователя устройства |
| • Финансовые данные<br>• Электронный кошелек<br>• Цифровые деньги<br>• Адрес криптографических хэш-функций<br>• Купон<br>• Государственный ID<br>• Водительское удостовер.<br>• Медицинская информация<br>• Список пациентов<br>• Электронное голосование<br>• Пенсия<br>• Информация однозначной идентификации и т.д. | • Физический ID доступ на основе определения местонахождения | • Смарт-карта для SSO<br>• Смартфон для SSO<br>• Смарт-карта SSO для облака<br>• Смартфон SSO для облака и т.д. | • аутентификация пользователя устройства в IoT устройстве<br>• аутентификация пользователя устройства в централизованном контроллере<br>• аутентификация пользователя устройства на сервере обслуживания IoT<br>• аутентификация пользователя устройства на сервере продавца IoT устройства |

Фиг. 13

20


Разнообразные комбинации биометрических данных
Комбинация 2 и более пальцев
Комбинация палец + радужная оболочка
Комбинация радужная оболочка + вена
Комбинация радужная оболочка + лицо
Комбинация палец + жест
Комбинация голос + лицо
Комбинация с каждым из ладонь / кровеносная система / голос / ДНК / нажатие клавиш и т.д.
Выделенные цели использования
Службы приложений
Банк / кредитная карта
Оплата
Государство
Интернет
Облако
Машина
IoT
911
Экстренная служба
Выделенные цели использования

Фиг. 14