РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 726 831** (13) **C1**

(51) МПК
H04L 29/06 (2006.01)
G06K 19/10 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 29/06 (2020.02); G06K 19/06037 (2020.02)

(21)(22) Заявка: **2019121938, 04.12.2017**

(24) Дата начала отсчета срока действия патента:
04.12.2017

Дата регистрации:
15.07.2020

Приоритет(ы):
(30) Конвенционный приоритет:
14.12.2016 CN 201611154671.9

(45) Опубликовано: **15.07.2020** Бюл. № **20**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **15.07.2019**

(86) Заявка PCT:
CN 2017/114382 (04.12.2017)

(87) Публикация заявки PCT:
WO 2018/107988 (21.06.2018)

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

(72) Автор(ы):
ШЭНЬ, Линнань (CN),
ЧЭНЬ, Гэ (CN),
ЛЮ, Янхой (CN),
ЦЗИНЬ, Хойфэн (CN)

(73) Патентообладатель(и):
АЛИБАБА ГРУП ХОЛДИНГ ЛИМИТЕД (KY)

(56) Список документов, цитированных в отчете о поиске: **RU 2195021 C1, 20.12.2002. US 2016/241405 A1, 18.08.2016. US 2012/308003 A1, 06.12.2012. US 2011/087596 A1, 14.04.2011.**

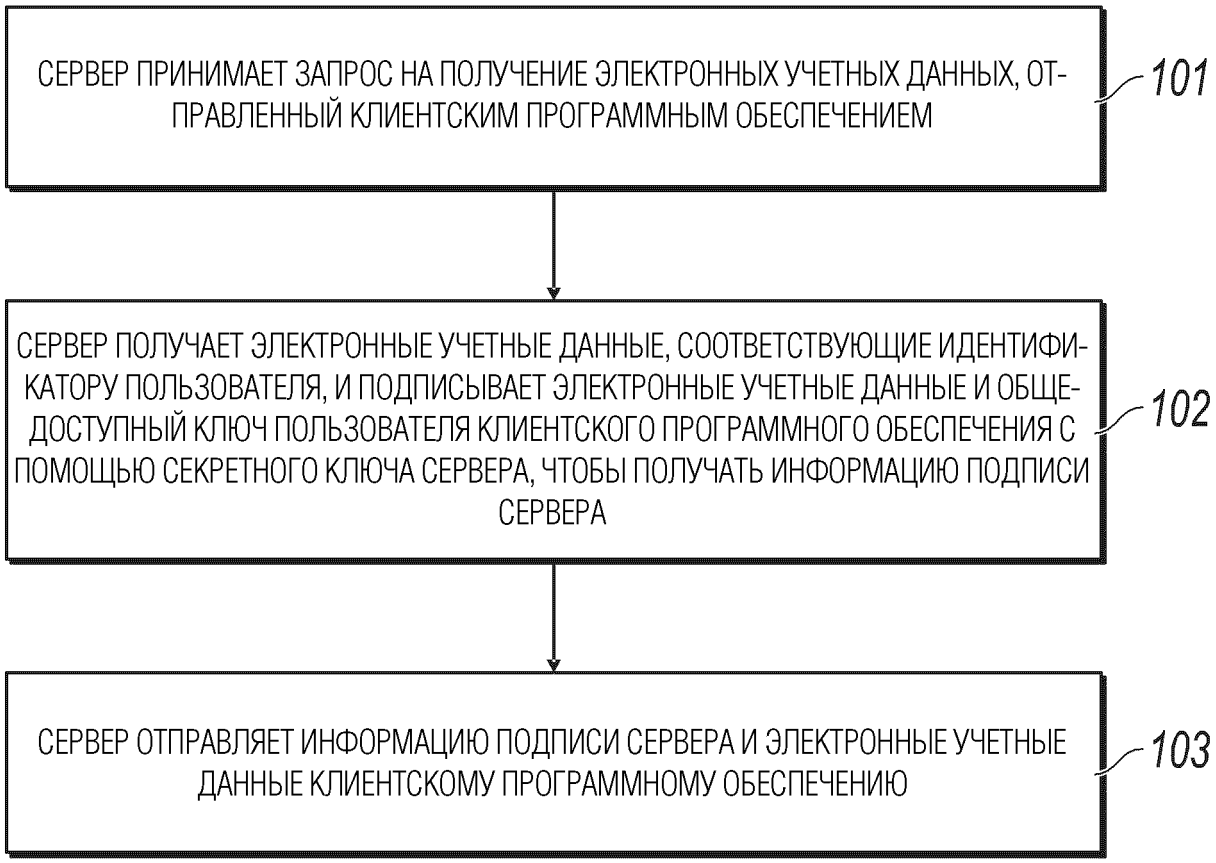
(54) СПОСОБ, ОБОРУДОВАНИЕ И СИСТЕМА ОБРАБОТКИ ДВУМЕРНЫХ ШТРИХ-КОДОВ

(57) Реферат:

Изобретение относится к области обработки информации и, в частности, к способу, устройству и системе обработки двумерных (2D) штрих-кодов. Технический результат заключается в защите обрабатываемых данных. Изобретение включает в себя сервер, принимающий запрос на получение электронного сертификата, переданный от клиента и содержащий идентификацию пользователя; сервер получает электронный сертификат, соответствующий идентификации пользователя, и использует секретный ключ сервера, чтобы подписывать электронный сертификат и общедоступный ключ пользователя на клиенте, чтобы получать информацию подписи сервера; и сервер передает клиенту информацию подписи сервера и электронный сертификат для клиента, чтобы выполнять проверку подписи в информации подписи сервера и формировать 2D штрих-код на основе электронного сертификата для терминала проверки сертификата для проверки электронного сертификата в 2D штрих-коде; причем терминал проверки сертификата формирует, в соответствии с идентификацией пользователя, электронный сертификат. 2 н. и 12 з.п. ф-лы. 14 ил.

RU 2726831 C1

RU 2726831 C1



ФИГ. 2

RU 2726831 C1

RU 2726831 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 726 831** (13) **C1**

(51) Int. Cl.
H04L 29/06 (2006.01)
G06K 19/10 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 29/06 (2020.02); G06K 19/06037 (2020.02)

(21)(22) Application: **2019121938, 04.12.2017**

(24) Effective date for property rights:
04.12.2017

Registration date:
15.07.2020

Priority:
(30) Convention priority:
14.12.2016 CN 201611154671.9

(45) Date of publication: **15.07.2020** Bull. № **20**

(85) Commencement of national phase: **15.07.2019**

(86) PCT application:
CN 2017/114382 (04.12.2017)

(87) PCT publication:
WO 2018/107988 (21.06.2018)

Mail address:
129090, Moskva, ul. B. Spasskaya, 25, str. 3, OOO "Yuridicheskaya firma Gorodisskij i Partnery"

(72) Inventor(s):
SHEN, Lingnan (CN),
CHEN, Ge (CN),
LIU, Yanghui (CN),
JIN, Huifeng (CN)

(73) Proprietor(s):
ALIBABA GROUP HOLDING LIMITED (KY)

RU 2726831 C1

(54) METHOD, EQUIPMENT AND SYSTEM FOR PROCESSING TWO-DIMENSIONAL BAR CODES

(57) Abstract:

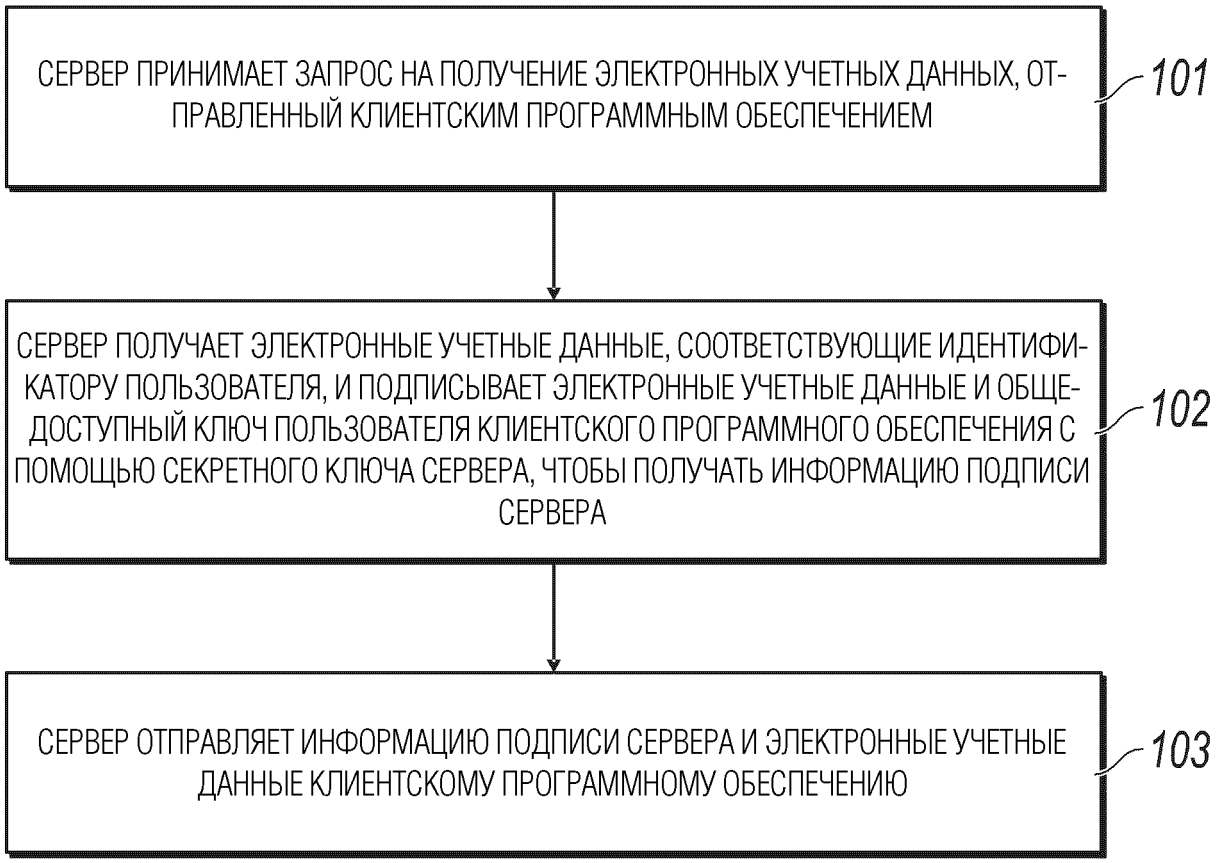
FIELD: data processing.

SUBSTANCE: invention relates to information processing and, in particular, to a method, apparatus and a system for processing two-dimensional (2D) barcodes. Invention includes a server receiving a request to receive an electronic certificate transmitted from a client and containing user identification; server receives an electronic certificate corresponding to user identification, and uses the server secret key to sign the electronic certificate and public key of the user on the client in order to obtain server signature information; and the server transmits to the client server signature information and an electronic certificate for the client to perform signature verification in the server signature information and generate 2D barcode based on the electronic certificate for the certificate verification terminal for verifying the electronic certificate in 2D barcode; wherein the certificate verification terminal generates an electronic certificate in accordance with the user identification.

EFFECT: technical result is protection of processed data.

14 cl, 14 dwg

RU 2726831 C1



ФИГ. 2

RU 2726831 C1

RU 2726831 C1

Область техники, к которой относится изобретение

[0001] Настоящее изобретение относится к области технологий обработки информации и, в частности, к способу, оборудованию и системе для обработки двумерных штрих-кодов.

Уровень техники

[0002] В настоящее время существует несколько сценариев применения проверки учетных данных в повседневной жизни и работе, например, удостоверение личности, банковская карта, билет на автобус, билет на концерт и карта контроля доступа. В некоторых сценариях применения проверка учетных данных должна выполняться только с использованием определенных объектов, например, билета на автобус, билета на концерт и карты контроля доступа. Для некоторых сценариев проверки учетных данных с относительно высокими требованиями к безопасности, конкретный объект и частная информация должны использоваться вместе для завершения проверки, например, банковская карта и доступ к дому/компании по отпечаткам пальцев.

[0003] На практике, в сценарии применения с проверкой учетных данных, который должен быть завершен только с использованием конкретного объекта, проверка учетных данных может быть завершена путем получения соответствующего конкретного объекта. Например, пользователь может купить бумажный билет на автобус или бумажный билет на концерт в билетном окне и может попасть на автобус или пойти на концерт после завершения проверки на турникете. Этот режим проверки зависит от конкретного объекта (билет на автобус или билет на концерт) и требует от пользователя носить конкретный объект. Однако, если конкретный объект будет потерян или поврежден, процесс отмены регистрации или последующей регистрации конкретного объекта является сложным.

[0004] Для сценария применения с требованием относительно высокой безопасности, безопасность может быть обеспечена с помощью дополнительного вспомогательного устройства аутентификации безопасности, например, защищенной клавиатуры или устройства распознавания отпечатков пальцев. Таким образом, стоимость использования увеличивается. Хотя этот способ может предотвратить утечку частной информации, угроза утечки частной информации по-прежнему существует.

[0005] В обоих предыдущих двух сценариях применения, существует проблема, что проверка учетных данных является менее удобной при относительно низкой безопасности, а стоимость стороны публикации учетных данных является относительно высокой. Для того, чтобы облегчать предыдущую задачу, пользователь в существующей технологии может купить электронные учетные данные онлайн. Строка случайных кодов записывается в электронные учетные данные и во время проверки учетных данных, проверка может быть выполнена путем проверки случайного кода в электронных учетных данных, тем самым повышая удобство и безопасность проверки учетных данных и снижения затраты на публикацию учетных данных. Тем не менее, в электронных учетных данных используется статический случайный код, и если электронные учетные данные копируются или украдены через фотографирование, безопасность электронных учетных данных не может быть обеспечена.

Сущность изобретения

[0006] В связи с этим, настоящее изобретение обеспечивает способ, оборудование и систему для обработки двумерных штрих-кодов и предназначено в основном для облегчения проблемы существующей технологии, что электронные учетные данные формируются на основе статического случайного кода, и когда электронные учетные данные однажды копируются или крадутся путем фотографирования, безопасность

электронных учетных данных не может быть обеспечена.

[0007] В соответствии с первым аспектом настоящего изобретения, настоящее изобретение предоставляет способ обработки двумерных штрих-кодов, включающий в себя следующее: прием, с помощью сервера, запроса на получение электронных учетных данных, отправленного клиентским программным обеспечением, где запрос на получение электронных учетных данных включает идентификатор пользователя; получение электронных учетных данных, которые соответствуют идентификатору пользователя, и подписание электронных учетных данных и общедоступного ключа пользователя клиентского программного обеспечения с использованием секретного ключа сервера для получения информации подписи сервера; и отправка информации подписи сервера и электронных учетных данных клиентскому программному обеспечению, так что клиентское программное обеспечение проверяет информацию подписи сервера и формирует двумерный штрих-код на основе электронных учетных данных, таким образом, что оконечное устройство проверки учетных данных проверяет электронные учетные данные, включенные в двумерный штрих-код, причем оконечное устройство проверки учетных данных сконфигурировано, чтобы формировать электронные учетные данные на основе идентификатора пользователя.

[0008] В соответствии со вторым аспектом настоящего изобретения, настоящее изобретение предоставляет способ обработки двумерных штрих-кодов, включающий в себя следующее: прием, с помощью клиентского программного обеспечения, информации подписи сервера и электронных учетных данных, которые отправляются сервером, где информация подписи сервера получается сервером путем подписания электронных учетных данных и общедоступного ключа пользователя клиентского программного обеспечения с помощью секретного ключа сервера; проверка информации подписи сервера, чтобы получать электронные учетные данные; получение ключа пользователя, который соответствует общедоступному ключу пользователя и подписание электронных учетных данных с помощью ключа пользователя для получения информации подписи клиентского программного обеспечения; и формирование двухмерного штрих-кода на основе заранее определенной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя, так что оконечное устройство проверки учетных данных проверяет электронные учетные данные, включенные в двумерный штрих-код на основе предварительно определенной информации безопасности и общедоступного ключа пользователя, причем предварительно определенная информация безопасности имеет продолжительность действия и оконечное устройство проверки учетных данных сконфигурировано, чтобы формировать электронные учетные данные на основе идентификатора пользователя.

[0009] В соответствии с третьим аспектом настоящего изобретения, настоящее изобретение предоставляет способ обработки двумерных штрих-кодов, включающий в себя следующее: получение оконечным устройством проверки учетных данных двумерного штрих-кода в клиентском программном обеспечении, в котором двумерный штрих-код формируется клиентским программным обеспечением на основе предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя, информация подписи клиентского программного обеспечения получается с помощью клиентского программного обеспечения путем подписания электронных учетных данных, и

информация подписи сервера получается сервером путем подписания электронных учетных данных и общедоступного ключа пользователя; проверка срока действия предварительно определенной информации безопасности, проверка информации подписи клиентского программного обеспечения и информации подписи сервера; если проверка каждой из предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения и информации подписи сервера прошла успешно, получение срока действия услуги, включенной в электронные учетные данные для проверки; и если проверка срока действия услуги, включенной в электронные учетные данные, прошла успешно, определение того, что проверка электронных учетных данных прошла успешно.

[0010] В соответствии с четвертым аспектом настоящего изобретения, настоящее изобретение предоставляет сервер, включающий в себя следующее: приемный блок, сконфигурированный, чтобы принимать запрос на получение электронных учетных данных, отправленный клиентским программным обеспечением, причем запрос на получение электронных учетных данных включает в себя идентификатор пользователя; первый блок получения, сконфигурированный для получения электронных учетных данных, которые соответствуют идентификатору пользователя, принятому приемным блоком; блок подписи, сконфигурированный для подписи электронных учетных данных и общедоступного ключа пользователя клиентского программного обеспечения с помощью секретного ключа сервера для получения информации подписи сервера; и блок отправки, сконфигурированный, чтобы отправлять информацию подписи сервера, полученную с помощью блока подписи, и электронные учетные данные, полученные первым блоком получения, клиентскому программному обеспечению, так что клиентское программное обеспечение проверяет информацию подписи сервера в течение срока действия ключа пользователя и формирует двумерный штрих-код на основе электронных учетных данных, таким образом, чтобы оконечное устройство проверки учетных данных проверяло электронные учетные данные, включенные в двумерный штрих-код, причем оконечное устройство проверки учетных данных сконфигурировано для формирования электронных учетных данных на основе идентификатора пользователя.

[0011] В соответствии с пятым аспектом настоящего изобретения, настоящее изобретение предоставляет клиентское программное обеспечение, включающее в себя следующее: первый приемный блок, сконфигурированный для приема информации подписи сервера и электронных учетных данных, которые отправляются сервером, где информация подписи сервера получается сервером путем подписания электронных учетных данных и общедоступного ключа пользователя клиентского программного обеспечения с помощью секретного ключа сервера; блок проверки подписи, сконфигурированный для проверки информации подписи сервера, чтобы получать электронные учетные данные; блок получения, сконфигурированный для получения ключа пользователя, который соответствует общедоступному ключу пользователя; блок подписи, сконфигурированный для подписания электронных учетных данных с помощью ключа пользователя, полученного блоком получения для получения информации подписи клиентского программного обеспечения; и блок формирования, сконфигурированный для формирования двумерного штрих-кода на основе предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя, так что оконечное устройство проверки учетных данных проверяет электронные учетные данные, включенные в

двумерный штрих-код, на основе предварительно определенной информации безопасности и общедоступного ключа пользователя, причем предварительно определенная информация безопасности имеет срок действия, и оконечное устройство проверки учетных данных сконфигурировано для формирования электронных учетных данных на основе идентификатора пользователя.

[0012] В соответствии с шестым аспектом настоящего изобретения, настоящее изобретение предоставляет оконечное устройство проверки учетных данных, включающее в себя следующее: первый блок получения, сконфигурированный для получения двумерного штрих-кода в клиентском программном обеспечении, где двумерный штрих-код формируется клиентским программным обеспечением на основе предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя, информация подписи клиентского программного обеспечения получается с помощью клиентского программного обеспечения путем подписания электронных учетных данных, и информация подписи сервера получается сервером путем подписания электронных учетных данных и общедоступного ключа пользователя; первый блок проверки, сконфигурированный для проверки срока действия предварительно определенной информации безопасности, полученной первым блоком получения; второй блок проверки, сконфигурированный для проверки информации подписи клиентского программного обеспечения и информации подписи сервера; третий блок проверки, сконфигурированный для получения срока действия услуги, включенной в электронные учетные данные для проверки, когда проверка первого блока проверки по предварительно определенной информации безопасности прошла успешно, проверка второго блока проверки по каждой информации подписи клиентского программного обеспечения и информации подписи сервере прошла успешно; и блок определения, сконфигурированный для определения того, что проверка электронных ученых данных завершается успешно, когда проверка третьего блока проверки на срок действия услуги, включенный в электронные учетные данные, прошла успешно.

[0013] В соответствии с седьмым аспектом настоящего изобретения, настоящее изобретение предоставляет систему для обработки двумерного штрих-кода и система включает в себя следующее: клиентское программное обеспечение, сконфигурированное для отправки запроса на получение электронных учетных данных на сервер, где запрос на получение электронных учетных данных включает в себя идентификатор пользователя; сервер, сконфигурированный для приема запроса на получение электронных учетных данных, отправленного клиентским программным обеспечением, и получения электронных учетных данных от оконечного устройства проверки учетных данных на основе идентификатора пользователя; и оконечное устройство проверки учетных данных, сконфигурированное для приема и ответа на запрос информации для получения электронных учетных данных, отправленного сервером, и отправки электронных учетных данных на сервер, причем сервер дополнительно сконфигурирован для приема электронных учетных данных, отправленных оконечным устройством проверки учетных данных, подписи электронных учетных данных и общедоступного ключа пользователя клиентского программного обеспечения, чтобы получать информацию подписи сервера, и отправки информации подписи сервера и электронных учетных данных клиентскому программному обеспечению; клиентское программное обеспечение, сконфигурированное для получения информации подписи сервера и электронных учетных данных, отправляемых сервером, проверки информации подписи

сервера, для получения электронных учетных данных, получения ключа пользователя, который соответствует общедоступному ключу пользователя, подписи электронных учетных данных с помощью ключа пользователя, чтобы получать информацию подписи клиентского программного обеспечения, и формирования двумерного штрих-кода на основе предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя; и оконечное устройство проверки учетных данных, сконфигурированное для получения двумерного штрих-кода в клиентском программном обеспечении, проверки срока действия предварительно определенной информации безопасности и проверки информации подписи клиентского программного обеспечения и информации подписи сервера; и если проверка по каждой из предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения и информации подписи сервера прошла успешно, получения срока действия услуги, включенного в электронные учетные данные для проверки и, если проверка на срок действия услуги, включенный в электронные учетные данные, прошла успешно, определения того, что проверка по электронным учетным данным прошла успешно.

[0014] В соответствии с предыдущими техническими решениями и в соответствии со способом, оборудованием и системой для обработки двумерных штрих-кодов, предусмотренных в настоящем изобретении, после приема запроса на получение электронных учетных данных, отправленного клиентским программным обеспечением, сервер подписывает электронные учетные данные и общедоступный ключ пользователя клиентского программного обеспечения с помощью секретного ключа сервера, чтобы получать информацию подписи сервера, и передает информацию подписи сервера и электронные учетные данные клиентскому программному обеспечению. Клиентское программное обеспечение принимает информацию подписи сервера и электронные учетные данные, которые отправляются сервером, проверяет информацию подписи сервера, после того как проверка информации подписи прошла успешно, подписывает электронные учетные данные и формирует двумерный штрих-код на основе предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя. После получения двумерного штрих-кода, оконечное устройство проверки учетных данных может проверять информацию подписи сервера, информацию подписи клиентского программного обеспечения и предварительно определенную информацию безопасности в двумерном штрих-коде, чтобы определять, были ли подделаны электронные учетные данные в процессе передачи, чтобы обеспечить безопасность электронных учетных данных в процессе использования.

[0015] Описание является лишь обзором технических решений настоящего изобретения. Чтобы более четко понимать технические средства настоящего изобретения для реализации содержимого спецификации и сделать более понятными предыдущие и другие цели, признаки и преимущества настоящего изобретения, ниже перечислены конкретные варианты реализации настоящего изобретения.

Краткое описание чертежей

[0016] Читая подробное описание следующих предпочтительных реализаций, специалист в данной области техники понимает различные другие преимущества и выгоды. Сопровождающие чертежи просто используются для того, чтобы показать цели предпочтительных реализаций, но не рассматриваются как ограничение настоящего

изобретения. Кроме того, одна и та же ссылочная позиция используется для обозначения одной и той же части на всех прилагаемых чертежах. На прилагаемых чертежах:

[0017] Фиг. 1 представляет собой основную схему, иллюстрирующую взаимодействие между клиентским программным обеспечением, сервером и оконечным устройством проверки учетных данных, в соответствии с осуществлением настоящего изобретения;

[0018] На фиг. 2 представляет собой блок-схему последовательности операций способа, иллюстрирующую первый способ для обработки двумерных штрих-кодов, в соответствии с осуществлением настоящего изобретения;

[0019] Фиг. 3 представляет собой блок-схему последовательности операций способа, иллюстрирующую второй способ для обработки двумерных штрих-кодов, в соответствии с осуществлением настоящего изобретения;

[0020] Фиг. 4 представляет собой блок-схему последовательности операций способа, иллюстрирующую третий способ для обработки двумерных штрих-кодов, в соответствии с осуществлением настоящего изобретения;

[0021] Фиг. 5 представляет собой схематичную диаграмму, иллюстрирующую подписание и проверку подписи, в соответствии с осуществлением настоящего изобретения;

[0022] Фиг. 6 представляет собой блок-схему последовательности операций способа, иллюстрирующую четвертый способ для обработки двумерных штрих-кодов, в соответствии с осуществлением настоящего изобретения;

[0023] Фиг. 7 представляет собой блок-схему последовательности операций способа, иллюстрирующую пятый способ для обработки двумерных штрих-кодов, в соответствии с осуществлением настоящего изобретения;

[0024] Фиг. 8 представляет собой принципиальную схему, иллюстрирующую сервер, в соответствии с осуществлением настоящего изобретения;

[0025] Фиг. 9 представляет собой принципиальную схему, иллюстрирующую другой сервер, в соответствии с осуществлением настоящего изобретения;

[0026] Фиг. 10 представляет собой принципиальную схему, иллюстрирующую клиентское программное обеспечение, в соответствии с осуществлением настоящего изобретения;

[0027] Фиг. 11 представляет собой принципиальную схему, иллюстрирующую другое клиентское программное обеспечение, в соответствии с осуществлением настоящего изобретения;

[0028] Фиг. 12 представляет собой принципиальную схему, иллюстрирующую оконечное устройство проверки учетных данных, в соответствии с осуществлением настоящего изобретения;

[0029] Фиг. 13 представляет собой принципиальную схему, иллюстрирующую другое оконечное устройство проверки учетных данных, в соответствии с осуществлением настоящего изобретения; а также

[0030] Фиг. 14 представляет собой принципиальную схему, иллюстрирующую систему для обработки двумерных штрих-кодов, в соответствии с осуществлением настоящего изобретения.

Описание реализаций

[0031] Последующее описывает примерные реализации настоящего изобретения более подробно со ссылкой на сопровождающие чертежи. Хотя прилагаемые чертежи показывают примерные реализации настоящего раскрытия, следует понимать, что настоящее раскрытие может быть реализовано в различных формах и не должно ограничиваться описанными здесь реализациями. Вместо этого эти реализации

предоставлены для того, чтобы специалист в данной области техники глубже понимал настоящее раскрытие и объем настоящего раскрытия.

[0032] Чтобы разрешить проблему существующей технологии, при которой электронные учетные данные в двумерном штрих-коде могут быть легко утеряны, варианты реализации настоящего изобретения обеспечивают способ обработки двухмерных штрих-кодов. Способ реализован на основе совместной работы сервера, клиентского программного обеспечения и оконечного устройства проверки учетных данных. Оконечное устройство проверки учетных данных может, по меньшей мере, формировать и передавать данные, чтобы передавать сформированные электронные учетные данные на сервер, и может получать данные и проверять данные, чтобы получать электронные учетные данные из двумерного штриха-кода в клиентском программном обеспечении, и проверять, являются ли электронные учетные данные верными. Сервер может, по меньшей мере, передавать и принимать данные, чтобы принимать электронные учетные данные, отправленные оконечным устройством проверки учетных данных, и отправлять электронные учетные данные на клиентское программное обеспечение, чтобы осуществлять передачу данных. Клиентское программное обеспечение может, по меньшей мере, обмениваться данными с сервером, чтобы принимать электронные учетные данные, отправленные сервером, и может формировать изображение, чтобы формировать двумерный штрих-код и т.д. на основе электронных учетных данных.

[0033] Перед тем как способ в реализации будет описан, для простоты понимания сначала представлена основная схема, иллюстрирующая взаимодействие между клиентским программным обеспечением, сервером и оконечным устройством проверки учетных данных, в соответствии с осуществлением настоящего изобретения, как это показано на фиг. 1. При осуществлении настоящего изобретения, после формирования электронных учетных данных на основе идентификатора пользователя (например, номера идентификационный карты, номера мобильного телефона или адреса электронной почты), оконечное устройство проверки учетных данных отправляет электронные учетные данные на сервер, и сервер имеет разрешение на доступ к электронным учетным данным, сформированным оконечным устройством проверки учетных данных. После приема запроса на получение электронных учетных данных от клиентского программного обеспечения, сервер отправляет электронные учетные данные в клиентское программное обеспечение, так что клиентское программное обеспечение формирует двумерный штрих-код на основе электронных учетных данных для проверки на оконечном устройстве проверки учетных данных.

[0034] Стоит отметить, что в этом варианте осуществления настоящего изобретения, описание производится с использованием в качестве примера того, что электронные учетные данные переносятся в двумерный штрих-код. Тем не менее, теоретически, электронные учетные данные могут также зависеть от другого носителя, например, клиентского программного обеспечения, которое имеет возможность NFC, такую как возможность SE или возможность HCE. При осуществлении настоящего изобретения, описание производится с использованием в качестве примера того, что электронные учетные данные переносятся в двумерный штрих-код, поскольку для пользователя электронных учетных данных и оконечного устройства проверки учетных данных двумерный штрих-код имеет относительно низкие требования к используемым аппаратным устройствам, и аппаратные устройства являются относительно универсальными. Тем не менее, должно быть ясно, что такой способ описания не предназначен, чтобы накладывать ограничение в том, что электронные учетные данные

могут существовать только при помощи двумерного штрих-кода.

[0035] Ниже первым представлен способ обработки двухмерных штрих-кодов, реализованный на стороне сервера, на основе принципиальной схемы, показанной на фиг. 1. Как показано на фиг. 2, способ включает в себя следующие этапы.

[0036] 101. Сервер принимает запрос на получение электронных учетных данных, отправленный клиентским программным обеспечением.

[0037] После успешного входа на сервер, клиентское программное обеспечение отправляет запрос на получение электронных учетных данных на сервер, где запрос на получение электронных учетных данных включает в себя идентификатор пользователя, так что сервер выполняет поиск соответствующих электронных учетных данных на основе идентификатора пользователя. В конкретном процессе реализации, электронные учетные данные могут включать в себя, но не ограничиваются следующим содержимым: электронные учетные данные, соответствующие авиабилету, билету на автобус, билету на поезд, билету на концерт, банковской карте, карте контроля доступа, входному билету в парк, удостоверению личности, купону на скидку, членскому билету, водительским правам, карте контроля доступа водительских прав или автобусной карте.

[0038] В конкретном процессе реализации, клиентское программное обеспечение является приложением (APP), установленным в электронном устройстве или на веб-сайте. Перед тем как клиентское программное обеспечение взаимодействует с сервером, клиентское программное обеспечение может зарегистрироваться на сервере на основе идентификатора пользователя, и идентификатор пользователя может включать в себя, но не ограничиваться, удостоверение личности пользователя, настоящее имя в соответствии с удостоверением личности, номер мобильного телефона, адрес электронной почты, имя учетной записи и т.д. В процессе регистрации может быть задан пароль для входа на сервер, а после регистрации и успешного входа клиентское программное обеспечение может быть подключено и взаимодействовать с сервером.

[0039] 102. Сервер получает электронные учетные данные, соответствующие идентификатору пользователя, и подписывает электронные учетные данные и общедоступный ключ пользователя клиентского программного обеспечения с помощью секретного ключа сервера, чтобы получать информацию подписи сервера.

[0040] Сервер, описанный в этом варианте осуществления настоящего изобретения, не формирует электронные учетные данные. После приема запроса на получение электронных учетных данных, отправленного клиентским программным обеспечением, сервер получает электронные учетные данные, которые соответствуют идентификатору пользователя, от оконечного устройства проверки учетных данных, которое формирует электронные учетные данные. Сервер действует в качестве моста между стороной, использующей электронные учетные данные (клиентское программное обеспечение), и оконечным устройством проверки электронных учетных данных (оконечное устройство проверки учетных данных), и несет ответственность за перенаправление электронных учетных данных, формируемых оконечным устройством проверки учетных данных, стороне, использующей электронные учетные данные. Стоит отметить, что при условии, что сервер, описанный в этой реализации настоящего изобретения, удовлетворяет национальным нормативным требованиям, сервер должен быть авторизован оконечным устройством проверки учетных данных для доступа к оконечному устройству проверки учетных данных.

[0041] Для того, чтобы предотвратить подделку электронных учетных данных в процессе передачи между сервером и клиентским программным обеспечением, до того,

как сервер отвечает на запрос на получение электронных учетных данных, отправленный клиентским программным обеспечением, сервер должен подписывать общедоступный ключ пользователя клиентского программного обеспечения, используя секретный ключ сервера, для получения информации подписи сервера. В этой реализации настоящего изобретения общедоступный ключ пользователя клиентского программного обеспечения подписан так, что клиентское программное обеспечение и сервер могут проверять идентичности друг друга, выполнять безопасную аутентификацию по идентификационной информации и гарантировать, что информация в процессе передачи данных не подделана. Сервер подписывает электронные учетные данные, используя секретный ключ сервера, чтобы можно было определить целостность исходных электронных учетных данных.

[0042] Кроме того, при подписании общедоступного ключа пользователя и электронных учетных данных сервер может дополнительно использовать информацию подписи сервера, полученную, когда сервер подписывает электронные учетные данные, и общедоступный ключ пользователя в качестве атрибута информации сформированного двумерного штрих-кода, когда клиентское программное обеспечение впоследствии формирует двумерный штрих-код, чтобы гарантировать, что электронные учетные данные, передаваемые клиентским программным обеспечением, отправляются сервером, проверяются клиентским программным обеспечением и являются авторизованными и надежными. Таким образом, электронные учетные данные не могут быть подделаны или аннулированы.

[0043] 103. Сервер отправляет информацию подписи сервера и электронные учетные данные клиентскому программному обеспечению.

[0044] Таким образом, клиентское программное обеспечение проверяет подписанные электронные учетные данные и формирует двумерный штрих-код на основе электронных учетных данных, так что оконечное устройство проверки учетных данных проверяет электронные учетные данные, включенные в двумерный штрих-код. Оконечное устройство проверки учетных данных сконфигурировано для формирования электронных учетных данных на основе идентификатора пользователя.

[0045] Согласно способу обработки двумерных штрих-кодов, представленному в этом варианте осуществления настоящего изобретения, после приема запроса на получение электронных учетных данных, отправленного клиентским программным обеспечением, сервер подписывает электронные учетные данные и общедоступный ключ пользователя клиентского программного обеспечения с помощью секретного ключа сервера, чтобы получать информацию подписи сервера, и передает информацию подписи сервера и электронные учетные данные клиентскому программному обеспечению. Клиентское программное обеспечение принимает информацию подписи сервера и электронные учетные данные, которые отправляются сервером, проверяет информацию подписи сервера, после того как проверка информации подписи прошла успешно, подписывает электронные учетные данные и формирует двумерный штрих-код на основе предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя. После получения двумерного штрих-кода, оконечное устройство проверки учетных данных может проверять информацию подписи сервера, информацию подписи клиентского программного обеспечения и предварительно определенную информацию безопасности в двумерном штрих-коде, чтобы определять, были ли подделаны электронные учетные данные в процессе передачи, чтобы обеспечить безопасность электронных учетных

данных в процессе использования.

[0046] В качестве дополнительного описания способа, показанного на фиг. 1, для обеспечения достоверности идентификатора пользователя клиентского программного обеспечения и обеспечения того, чтобы идентификатор пользователя клиентского программного обеспечения не был подделан в процессе передачи содержимого, на этапе 102 электронные учетные данные и общедоступный ключ пользователя клиентского программного обеспечения могут быть подписаны с использованием секретного ключа сервера следующими способами. Например:

[0047] Способ 1: Сервер выделяет ключ подписи пользователя электронным учетным данным и подписывает электронные учетные данные и первый общедоступный ключ пользователя с помощью секретного ключа сервера, причем выделенный ключ подписи пользователя включает в себя первый общедоступный ключ пользователя.

[0048] Когда сервер принимает запрос на получение электронных учетных данных, отправленный клиентским программным обеспечением, если нет общедоступного ключа пользователя клиентского программного обеспечения, полученного из запроса на получение электронных учетных данных, сервер временно выделяет пары ключей подписи пользователя электронным учетным данным, чтобы аутентифицировать идентификатор пользователя клиентского программного обеспечения и, следовательно, гарантировать, что электронные учетные данные не были подделаны, причем выделенные ключи подписи пользователя включают в себя один первый общедоступный ключ пользователя и один первый секретный ключ пользователя; и подписывает первый секретный ключ пользователя, используя секретный ключ сервера, чтобы выполнять безопасную аутентификацию по информации подписи сервера после приема информации подписи сервера.

[0049] Поскольку ключи подписи пользователя временно выделяются сервером для электронных учетных данных, если ключи подписи пользователя не получены клиентским программным обеспечением, информация подписи сервера на сервере не может быть проверена. Чтобы облегчать предыдущую проблему, если сервер подписывает электронные учетные данные и первый общедоступный ключ пользователя клиентского программного обеспечения с использованием способа 1, то когда сервер отправляет информацию подписи сервера и электронные учетные данные клиентскому программному обеспечению, сервер должен синхронно отправлять ключи подписи пользователя, выделенные электронным учетным данным, клиентскому программному обеспечению, чтобы клиентское программное обеспечение могло проверять информацию подписи сервера на основе ключей подписи пользователя.

[0050] В конкретном процессе реализации, после приема ключей подписи пользователя, временно выделенных сервером электронным учетным данным, и проверки информации подписи сервера на основе ключей подписи пользователя, клиентское программное обеспечение может напрямую отказаться от ключей подписи пользователя или может использовать ключи подписи пользователя как общие ключи пользователя и общедоступные ключи пользователя клиентского программного обеспечения. Реализации не ограничены в этом осуществлении настоящего изобретения.

[0051] Способ 2: Сервер получает второй общедоступный ключ пользователя, отправленный клиентским программным обеспечением, и подписывает второй общедоступный ключ пользователя и электронные учетные данные с помощью секретного ключа сервера.

[0052] В этой реализации, чтобы идентифицировать идентификатор клиентского программного обеспечения, при отправке запроса на получение электронных учетных

данных на сервер клиентское программное обеспечение синхронно отправляет второй общедоступный ключ пользователя клиентского программного обеспечения на сервер, так что сервер выполняет аутентификацию идентификации по клиентскому программному обеспечению, и сервер подписывает второй общедоступный ключ пользователя и электронные учетные данные клиентского программного обеспечения, используя секретный ключ сервера. После приема подписанного второго общедоступного ключа пользователя и подписанных электронных учетных данных клиентское программное обеспечение может получать информацию электронных учетных данных только после успешной проверки подписи, чтобы гарантировать, что электронные учетные данные не были подделаны.

[0053] Стоит отметить, что первый общедоступный ключ пользователя и второй общедоступный ключ пользователя, описанные в этой реализации настоящего изобретения, используются для различения различных общедоступных ключей пользователя клиентского программного обеспечения. "Первый" и "второй" не имеют других значений и не предназначены для ограничения числа, приоритета и т.д. общедоступных ключей пользователя. Способ именования общедоступного ключа пользователя в клиентском программном обеспечении не ограничен в этой реализации настоящего изобретения.

[0054] Для простоты описания, в последующем описании в осуществлении настоящего изобретения, описание производится с использованием, например, того, что общедоступный ключ пользователя и секретный ключ пользователя являются асимметричными ключами. Однако должно быть ясно, что общедоступный ключ пользователя и секретный ключ пользователя не ограничиваются асимметричными ключами, и могут быть симметричными ключами. Реализации не ограничены в этом осуществлении настоящего изобретения.

[0055] Для облегчения понимания процесса подписи сервера, далее для описания используется пример, что сервер подписывает общедоступный ключ пользователя и электронные учетные данные. Конкретный процесс включает в себя следующее: После получения общедоступного ключа пользователя и электронных учетных данных, сервер может выполнять операцию хеширования общедоступного ключа пользователя и электронных учетных данных с использованием алгоритма хеширования для получения значения хеш-функции, а затем подписывать значение хеш-функции, используя секретный ключ сервера для получения информации подписи сервера. Алгоритм (например, операция хеширования), используемый в процессе подписи, не ограничивается в этом варианте осуществления настоящего изобретения.

[0056] После подписания электронных учетных данных и общедоступного ключа пользователя сервер отправляет электронные учетные данные, подписанный общедоступный ключ пользователя и подписанные электронные учетные данные клиентскому программному обеспечению, чтобы клиентское программное обеспечение проверило информацию подписи сервера и гарантировало, что электронные учетные данные не подделаны в злоумышленником в процессе передачи данных. Кроме того, серверу дополнительно необходимо распространить общедоступный ключ, соответствующий секретному ключу сервера, который используется, когда сервер получает информацию подписи, чтобы клиентское программное обеспечение и оконечное устройство проверки учетных данных приняли общедоступный ключ, распространенный сервером, и использовали общедоступный ключ сервера для проверки информации подписи.

[0057] Дополнительно сервер, описанный в этом варианте осуществления настоящего

изобретения, служит мостом, который связывает клиентское программное обеспечение и сторону проверки учетных данных. Сервер отвечает за аутентификацию достоверности пользователя и, кроме того, сервер может дополнительно проверять достоверность использования электронных учетных данных. В конкретных процессах использования электронные учетные данные соответствуют различным типам услуг, а различные типы услуг ограничены использованием различных спецификаций услуг. Например, когда электронные учетные данные являются авиабилетом, услуга авиабилета включает в себя время отправления самолета (этот сценарий применения может быть только сценарием с самолетом, который вылетает вовремя, без задержки). В качестве альтернативы, когда электронные учетные данные являются билетом на концерт, услуга билета также включает в себя время начала, время входа и т.д. концерта. Следовательно, в этой реализации настоящего изобретения перед получением соответствующих электронных учетных данных на основе идентификатора пользователя серверу необходимо проанализировать запрос на получение электронных учетных данных, получать время действия услуг, включенное в запрос на получение электронных учетных данных, и проверять, соответствует ли время действия услуг спецификации услуг. Когда время действия услуги соответствует спецификации услуги, сервер получает электронные учетные данные, которые соответствуют идентификатору пользователя. Когда срок действия услуги не соответствует спецификации услуги, сервер возвращает клиентскому программному обеспечению оперативную информацию, указывающую, что соответствующие электронные учетные данные недоступны.

[0058] Для лучшего понимания ниже приведено описание срока действия услуги и спецификации услуг с примерами. Например, предположим, что электронные учетные данные являются услугой автобусных билетов, для оконечного устройства проверки учетных данных время предварительной продажи автобусных билетов определено 7 дней, а текущая дата 1 ноября 2016. Пользователь отправляет запрос на получение электронных учетных данных на сервер с помощью клиентского программного обеспечения 1 ноября 2016 года, время действия услуги, включенное в запрос, 20 ноября 2016 года, и максимальное время действия электронных учетных данных, формируемых оконечным устройством проверки учетных данных - до 8 ноября 2016 года. Таким образом, сервер может определять, что время действия услуги не соответствует в спецификации услуги. Предшествующее описание является лишь примером. Эта реализация настоящего изобретения не накладывает никаких ограничений на тип услуги электронных учетных данных, на время действия услуги, на спецификации услуги и т.д.

[0059] Дополнительно на этапе 102 электронные учетные данные, которые соответствуют идентификатору пользователя, могут быть получены следующими способами, но не ограничиваются этими способами. Например:

[0060] Способ 1: После того, как оконечное устройство проверки учетных данных формирует электронные учетные данные на основе идентификатора пользователя, учетные данные, синхронизированные оконечным устройством проверки учетных данных, принимаются.

[0061] В этой реализации после формирования электронных учетных данных оконечное устройство проверки учетных данных активно отправляет сформированные электронные учетные данные на сервер. В конкретном процессе реализации, чтобы облегчать управление множеством электронных учетных данных, сервер может формировать локально предварительно определенный список, причем предварительно определенный список используется для записи сопоставления между идентификатором пользователя и электронными учетными данными. После приема электронных учетных

данных, синхронизированных оконечным устройством проверки учетных данных, сервер записывает недавно принятое сопоставление между электронными учетными данными и идентификатором пользователя в предварительно определенный список. После отправки электронных учетных данных клиентскому программному обеспечению, сервер может удалять электронные учетные данные, которые были успешно отправлены из предварительно определенного списка, чтобы сокращать ресурсы, занимаемые сервером.

[0062] Способ 2: Запрос информации для получения электронных учетных данных отправляется на оконечное устройство проверки учетных данных на основе идентификатора пользователя, чтобы получать электронные учетные данные.

[0063] В этой реализации сервер используется для пересылки. Сервер запрашивает электронные учетные данные от оконечного устройства проверки учетных данных на основе идентификатора пользователя в запросе на получение электронных учетных данных только в случае приема запроса на получение электронных учетных данных, отправленного клиентским программным обеспечением, а затем пересылает полученные электронные учетные данные в клиентское программное обеспечение. Способ получения электронных учетных данных сервером не ограничивается в этом варианте осуществления настоящего изобретения.

[0064] Дополнительно, как далее описано и в продолжении предыдущего способа, реализация настоящего изобретения дополнительно предоставляет способ обработки двумерных штрих-кодов. В способе, для простоты описания, описание в основном производится с использованием в качестве примера того, что клиентским программным обеспечением является ALIPAY и электронные учетные данные являются электронным билетом на концерт. Должно быть понятно, что такие способы описания не предназначены, чтобы накладывать ограничение на то, что клиентское программное обеспечение, описанное в этом варианте осуществления настоящего изобретения, может быть только ALIPAY. Как показано на фиг. 3, способ включает в себя следующие этапы.

[0065] 201. Сервер принимает запрос на получение электронного билета на концерт, отправленного ALIPAY, где запрос на получение электронного билета на концерт включает в себя номер мобильного телефона и срок действия услуги.

[0066] На практике сроком действия услуги может быть время бронирования электронного билета на концерт, или может быть время начала электронного билета на концерт, или может быть любое время, не связанное с электронным билетом на концерт. Срок действия услуги не ограничен в этой реализации настоящего изобретения.

[0067] 202a. Сервер анализирует запрос на получение электронного билета на концерт и получает срок действия услуги, включенный в запрос на получение электронного билета на концерт.

[0068] Например, срок действия услуги в запросе - это время начала концерта: 16:00 20 сентября 2016 года, а текущая дата - 1 сентября 2016 года.

[0069] 203a. Проверяется, соответствует ли срок действия услуги спецификации услуги.

[0070] Если срок действия услуги соответствует спецификации услуги, выполняется этап 204. Если срок действия услуги не соответствует спецификации услуги, выполняется этап 205.

[0071] В этом варианте осуществления настоящего изобретения, электронный билет на концерт получается по следующему сценарию: Когда бумажный билет на концерт потерян или поврежден, вход на концерт может быть выполнен путем проверки электронного билета на концерт, без пост-регистрации бумажного билета на концерт. Это сокращает утомительный процесс пост-регистрации билета. В этом примере можно

указать, что спецификацией услуги является то, что электронный билет на концерт можно получить в течение 30 дней до открытия концерта или электронный билет на концерт можно получить в течение получаса после открытия концерта. Этап 202b может быть выполнен при условии, что срок действия услуги соответствует спецификации услуги. Срок действия, описанный на этапе 201, является временем начала концерта 20 сентября 2016 года, которое соответствует спецификации услуги, поэтому выполняется этап 202b.

[0072] 202b. Сервер анализирует запрос на получение электронного билета на концерт и получает номер мобильного телефона в запросе на получение электронного билета на концерт.

[0073] 203b. Проверяется достоверность номера мобильного телефона.

[0074] Если номер мобильного телефона достоверен, выполняется этап 204. Если номер мобильного телефона недостоверен, выполняется этап 205.

[0075] На данном этапе проверяется, соответствует ли номер мобильного телефона в запросе номеру мобильного телефона на сервере.

[0076] Стоит отметить, что, когда этап 202a и этап 202b выполняются, между этими двумя этапами нет последовательности. Кроме того, последующие шаги продолжают выполняться только после того, как проверка по сроку действия услуги и проверка по идентификатору пользователя (номеру мобильного телефона) прошли успешно.

[0077] 204. Сервер получает электронный билет на концерт, который соответствует номеру мобильного телефона и подписывает общедоступный ключ пользователя из ALIPAY и электронные учетные данные, используя секретный ключ сервера, для получения информации подписи сервера.

[0078] Основанные на различных типах услуг, электронные учетные данные имеют соответствующие детали. Электронный билет на концерт используется в качестве примера. Электронный билет на концерт включает в себя место концерта, трибуну, конкретный номер места, название концерта, цену и т.д. Реализации не ограничены в этом осуществлении настоящего изобретения.

[0079] 205. Перехватывается запрос на приобретение электронного билета на концерт и отправляется подсказка на отказ в запросе в ALIPAY.

[0080] 206. Отправка информации подписи сервера и электронного билета на концерт в ALIPAY.

[0081] 207. Распространение общедоступного ключа, который соответствует секретному ключу сервера, так что ALIPAY проверяет информацию подписи на основе общедоступного ключа сервера.

[0082] Как расширение к способу, показанному на фиг. 3, после того, как электронное устройство (например, мобильный телефон), с установленным ALIPAY, потеряно, пользователь может переключить мобильный телефон и, после успешного входа в ALIPAY, продолжать использовать электронные учетные данные, избегая отмены регистрации, пост-регистрации и т.д. после того, как бумажные учетные данные потеряны. Такой сценарий применения может применяться только после того, как ALIPAY выполнил успешную проверку подписи с помощью секретного ключа пользователя, общедоступного ключа сервера и электронных учетных данных. Если ALIPAY не проверяет информацию подписи сервера, ALIPAY необходимо проверять информацию подписи сервера на основе общедоступного ключа сервера и получать электронные учетные данные после того, как проверка прошла успешно. В необязательном осуществлении настоящего изобретения, для дополнительного определения, что электронные учетные данные не утеряны, после того как сервер

отправляет информацию подписи сервера и электронные учетные данные клиентскому программному обеспечению, может быть установлен период действия проверки для общедоступного ключа сервера. Таким образом, клиентское программное обеспечение должно завершить проверку информации подписи сервера в течение указанного срока. Если период действия проверки для общедоступного ключа сервера истекает, информация подписи сервера не может быть проверена.

[0083] Дополнительно реализация настоящего изобретения дополнительно предоставляет способ обработки двумерных штрих-кодов. Способ применяется к стороне клиентского программного обеспечения, показанной на фиг. 1. Как показано на фиг. 4, способ включает в себя следующие этапы.

[0084] 301. Клиентское программное обеспечение принимает информацию подписи сервера и электронные учетные данные, которые отправляются сервером.

[0085] После того, как клиентское программное обеспечение успешно входит на сервер, используя имя учетной записи пользователя и пароль входа в систему, клиентское программное обеспечение отправляет запрос на получение электронных учетных данных на сервер. Сервер отвечает на запрос на получение электронных учетных данных. Для того, чтобы предотвратить подделку электронных учетных данных в процессе передачи, сервер отправляет информацию подписи сервера и электронные учетные данные клиентскому программному обеспечению, для проверки достоверности идентификации клиентского программного обеспечения. Информация подписи сервера получается сервером путем подписания электронных учетных данных и общедоступного ключа пользователя клиентского программного обеспечения, используя секретный ключ сервера. Для связанных описаний получения информации подписи сервера могут быть сделаны ссылки на подробные описания в предыдущей реализации. Подробности опущены для простоты в этом осуществлении настоящего изобретения.

[0086] 302. Клиентское программное обеспечение проверяет информацию подписи сервера, чтобы получать электронные учетные данные.

[0087] Например, информация подписи сервера, полученная путем подписания общедоступного ключа пользователя и электронных учетных данных сервером, и проверка информации подписи сервера, выполняемая с помощью клиентского программного обеспечения, используются как пример для подробного описания. Фиг. 5 представляет собой схематичную диаграмму, иллюстрирующую подписание и проверку подписи, в соответствии с осуществлением настоящего изобретения. После получения общедоступного ключа пользователя и электронных учетных данных, сервер выполняет операцию хеширования общедоступного ключа пользователя и электронных учетных данных с использованием алгоритма хеширования для получения первого значения хеш-функции и шифрует первое значение хеш-функции с помощью секретного ключа сервера, чтобы получать информацию подписи сервера. Сервер отправляет информацию подписи сервера и электронные учетные данные клиентскому программному обеспечению. После приема информации подписи сервера и электронной учетных данных клиентское программное обеспечение извлекает электронные учетные данные и выполняет операцию хеширования электронных учетных данных, чтобы получать второе значение хеш-функции. Кроме того, клиентское программное обеспечение использует общедоступный ключ сервера для расшифровки информации подписи сервера, чтобы получать первое значение хеш-функции, и сравнивает первое значение хеш-функции, полученное путем дешифрования, со вторым значением хеш-функции, полученное расчетным путем. Если первое значение хеш-функции совпадает со вторым значением хеш-функции, это указывает на то, что электронные учетные данные не были

подделаны в процессе передачи, и электронные учетные данные могут использоваться непосредственно после получения электронных учетных данных. Если первое значение хеш-функции отличается от второго значения хеш-функции, это указывает на то, что электронные учетные данные были подделаны в процессе передачи данных, и может быть риск утечки информации. Стоит отметить, что фиг. 5 является только примером, и конкретное содержимое информации подписи сервера не ограничено.

[0088] 303. Клиентское программное обеспечение получает ключ пользователя, соответствующий общедоступному ключу пользователя, и подписывает электронные учетные данные с помощью ключа пользователя для получения информации подписи клиентского программного обеспечения.

[0089] Клиентское программное обеспечение формирует электронные учетные данные, которые приводятся в двумерный штрих-код. Для того, чтобы предотвратить незаконную подделку электронных учетных данных и предотвратить утечку информации электронных учетных данных, клиентское программное обеспечение должно подписывать электронные учетные данные, используя секретный ключ пользователя, чтобы получать информацию подписи клиентского программного обеспечения. Когда клиентское программное обеспечение использует информацию подписи клиентского программного обеспечения в качестве информации атрибута сформированного двумерного штрих-кода, оконечное устройство проверки учетных данных может проверять информацию подписи клиентского программного обеспечения и дополнительно аутентифицирует достоверность клиентского программного обеспечения.

[0090] Для конкретной реализации способа подписи, ссылки могут быть сделаны к подробному описанию на фиг. 5. Подробности опущены для простоты в этом осуществлении настоящего изобретения.

[0091] 304. Клиентское программное обеспечение формирует двумерный штрих-код на основе предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя.

[0092] Когда клиентское программное обеспечение и сторона проверки учетных данных выполняют передачу данных (электронные учетные данные) на короткие расстояния, чтобы обеспечивать безопасность передачи электронных учетных данных, информация аутентификации может быть добавлена к сформированному двумерному штрих-коду, и информация аутентификации может включать в себя, но не ограничивается этим, информацию подписи клиентского программного обеспечения, информацию подписи сервера и предварительно определенную информацию безопасности. Оконечное устройство проверки учетных данных может проверять информацию подписи клиентского программного обеспечения, чтобы определять, что электронные учетные данные, которые необходимо проверять, отправлены клиентским программным обеспечением. Кроме того, оконечное устройство проверки учетных данных может проверять информацию подписи сервера, чтобы определять, что электронные учетные данные в двумерном штрих-коде отправлены сервером, чтобы гарантировать, что электронные учетные данные не были подделаны.

[0093] В этой реализации настоящего изобретения предварительно заданная информация безопасности используется в качестве динамической реализации двумерного штрих-кода и используется в качестве учетных данных для установления "достоверной" передачи данных между клиентским программным обеспечением и оконечным устройством проверки учетных данных. Перед приемом двумерного штрих-кода, отправленного клиентским программным обеспечением, оконечное устройство проверки

учетных данных проверяет достоверность и безопасность предварительно заданной информации безопасности, чтобы обеспечить безопасность электронных учетных данных, отправленных клиентским программным обеспечением. Предварительно заданная информация безопасности может включать в себя, но не ограничивается следующим содержимым: информацию динамического пароля, информацию времени, информацию произвольного кода и т.д. Реализации не ограничены в этом осуществлении настоящего изобретения.

[0094] Например, как описано здесь, текущее системное время используется для предварительно заданной информации безопасности. Если клиентское программное обеспечение формирует двумерный штрих-код в 08:00, может быть определено, что предварительно заданная информация безопасности представляет собой 08/00. Если клиентское программное обеспечение формирует двумерный штрих-код в 10:21, может быть определено, что предварительно заданная информация безопасности представляет собой 10/21. Предыдущий пример описывается с использованием предварительно заданной информации безопасности в качестве текущего системного времени. Тем не менее, должно быть ясно, что такие способы описания не предназначены для того, чтобы накладывать ограничение, что предварительно заданной информацией безопасности, описанной в этом варианте осуществления настоящего изобретения, может быть только текущее системное временем клиентского программного обеспечения.

[0095] Стоит отметить, что когда формируется двумерный штрих-код, общедоступный ключ пользователя клиентского программного обеспечения не распространяется, и вместо этого общедоступный ключ пользователя непосредственно используется в качестве информации атрибута сформированного двумерного штрих-кода. Это может эффективно уменьшить дополнительные накладные расходы и стоимость клиентского программного обеспечения.

[0096] Согласно способу обработки двумерных штрих-кодов, представленному в этом варианте осуществления настоящего изобретения, после приема запроса на получение электронных учетных данных, отправленного клиентским программным обеспечением, сервер подписывает электронные учетные данные и общедоступный ключ пользователя клиентского программного обеспечения с помощью секретного ключа сервера, чтобы получать информацию подписи сервера, и передает информацию подписи сервера и электронные учетные данные клиентскому программному обеспечению. Клиентское программное обеспечение принимает информацию подписи сервера и электронные учетные данные, которые отправляются сервером, проверяет информацию подписи сервера, после того как проверка информации подписи прошла успешно, подписывает электронные учетные данные и формирует двумерный штрих-код на основе предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя. После получения двумерного штрих-кода, оконечное устройство проверки учетных данных может проверять информацию подписи сервера, информацию подписи клиентского программного обеспечения и предварительно определенную информацию безопасности в двумерном штрих-коде, чтобы определять, были ли подделаны электронные учетные данные в процессе передачи, чтобы обеспечить безопасность электронных учетных данных в процессе использования.

[0097] В реализации настоящего изобретения, при получении ключа пользователя, который соответствует общедоступному ключу пользователя, клиентское программное

обеспечение принимает ключ подписи пользователя, который отправлен сервером и который выделен для электронных учетных данных, причем ключ подписи пользователя включает в себя первый общедоступный ключ пользователя и первый ключ пользователя, ключ пользователя и общедоступный ключ пользователя являются асимметричными ключами, и клиентское программное обеспечение получает первый ключ пользователя в ключе подписи пользователя, выделенном сервером для электронных учетных данных. В другом варианте осуществления настоящего изобретения, при получении ключа пользователя, который соответствует общедоступному ключу пользователя, клиентское программное обеспечение может получать второй ключ пользователя, который формируется с помощью клиентского программного обеспечения и который соответствует общедоступному ключу пользователя. Способ для клиентского программного обеспечения для получения ключа пользователя не ограничен в этой реализации настоящего изобретения.

[0098] Дополнительно при проверке информации подписи сервера, способ включает в себя следующее: прием и хранение общедоступного ключа сервера, распространенного сервером, и проверка информации подписи сервера на основе общедоступного ключа сервера и электронных учетных данных.

[0099] При определении того, что сервер подписывает второй общедоступный ключ пользователя, сформированный клиентским программным обеспечением, клиентское программное обеспечение проверяет информацию подписи сервера на основе общедоступного ключа сервера, электронных учетных данных и первого общедоступного ключа пользователя.

[0100] При определении того, что сервер подписывает первый общедоступный ключ пользователя, выделенный сервером для электронных учетных данных, клиентское программное обеспечение проверяет информацию подписи сервера на основе общедоступного ключа сервера, электронных учетных данных и второго общедоступного ключа пользователя. Для процесса, в котором клиентское программное обеспечение проверяет информацию подписи сервера, ссылки могут быть сделаны к подробному описанию на фиг. 5. Реализации не ограничены в этом осуществлении настоящего изобретения.

[0101] Стоит отметить, что, при отправке электронных учетных данных клиентскому программному обеспечению, сервер должен подписывать электронные учетные данные и общедоступный ключ пользователя, чтобы получать информацию подписи сервера, чтобы при последующем формировании клиентским программным обеспечением двумерного штрих-кода информация подписи сервера могла использоваться как информация атрибута сформированного двумерного штрих-кода. Пользователь использует секретный ключ пользователя, чтобы подписывать информацию, отправляемую на сервер, чтобы гарантировать правильность исходной информации электронных учетных данных и гарантировать, что общедоступный ключ пользователя является действительным и надежным, как проверенный, и не может быть подделан или отвергнут.

[0102] Дополнительно может быть множество ключей подписи пользователя (в том числе первый ключ пользователя, сформированный клиентским программным обеспечением, и второй ключ пользователя, выделенный сервером для электронных учетных данных) в клиентском программном обеспечении. Следовательно, клиентское программное обеспечение может подписывать электронные учетные данные с помощью любого секретного ключа пользователя, который соответствует клиентскому программному обеспечению. Например, клиентское программное обеспечение может

подписывать электронные учетные данные с помощью первого ключа пользователя или может подписывать электронные учетные данные с помощью второго ключа пользователя. Реализации не ограничены в этом осуществлении настоящего изобретения.

[0103] Для дополнительного обеспечения безопасности электронных учетных данных, когда клиентское программное обеспечение формирует двумерный штрих-код, клиентское программное обеспечение также использует информацию подписи клиентского программного обеспечения в процессе. Таким образом, оконечное устройство проверки учетных данных проверяет информацию подписи клиентского программного обеспечения, чтобы гарантировать, что электронные учетные данные сформированы клиентским программным обеспечением, и клиентское программное обеспечение авторизовано и надежно для использования электронных учетных данных, а электронные учетные данные не могут быть подделаны или аннулированы. Двумерный штрих-код может быть сформирован на основе предварительно заданной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя следующим способом: установка периода действия предварительно заданной информации безопасности и формирование двумерного штрих-кода на основе предварительно заданной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных, общедоступного ключа пользователя, периода действия предварительно заданной информации безопасности и идентификатора пользователя.

[0104] Стоит отметить, что в этой реализации настоящего изобретения при формировании двумерного штрих-кода клиентскому программному обеспечению необходимо использовать идентификатор пользователя в качестве информации атрибута сформированного двумерного штрих-кода. Это может быть применено к сценарию применения с оконечным устройством проверки учетных данных, требующим систему реального имени пользователя. Например, когда электронные учетные данные являются учетными данными, которые соответствуют авиабилету, билету на автобус, билету на поезд, банковской карте и т.д., когда оконечное устройство проверки учетных данных проверяет такие электронные учетные данные, удостоверение личности пользователя может использоваться для проверки состояния системы реального имени, чтобы помогать в завершении проверки, чтобы удовлетворять требованию в некоторых сценариях приложений, требующих систему реального имени.

[0105] В дополнительном решении в этом варианте осуществления настоящего изобретения, в некоторых сценариях с высоким уровнем безопасности, когда двумерный штрих-код формируется, чтобы предотвращать использование злоумышленником двумерного штрих-кода, когда мобильный телефон или планшетный компьютер теряются, или в течение короткого периода времени, когда двумерный штрих-код взломан, биометрический признак человека, использующего электронные учетные данные, может быть добавлен к двумерному штрих-коду. Например, биометрический признак, такой, как отпечаток пальца человека, использующего электронные учетные данные, включен в двумерный штрих-код. Когда оконечное устройство проверки учетных данных проверяет двумерный штрих-код, необходима проверка биометрического признака человека для дополнительного обеспечения безопасности электронных учетных данных.

[0106] Дополнительно в предыдущей реализации подробно описаны конкретные функции и конкретные реализации сервера и клиентского программного обеспечения для обработки двумерного штрих-кода. Оконечное устройство проверки учетных

данных, показанное на фиг. 1, должно выполнять проверку сформированных электронных учетных данных, которые зависят от двумерного штрих-кода. Ниже приводится способ обработки двумерных штрих-кодов. Способ применяется к оконечному устройству проверки учетных данных. Как показано на фиг. 6, способ включает в себя следующие этапы.

[0107] 401. Оконечное устройство проверки учетных данных получает двумерный штрих-код в клиентском программном обеспечении.

[0108] Двумерный штрих-код формируется клиентским программным обеспечением на основе предварительно заданной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя, информация подписи клиентского программного обеспечения получается с помощью клиентского программного обеспечения путем подписания электронных учетных данных и информация подписи сервера получается с помощью сервера путем подписания электронных учетных данных и общедоступного ключа пользователя.

[0109] Оконечное устройство проверки учетных данных может получать двумерный штрих-код в клиентском программном обеспечении следующим способом и т.д. Например, двумерный штрих-код, полученный при использовании предварительно заданной инструкции получения данных. Способы, связанные с предварительно заданной инструкцией получения данных включают в себя способ сканирования, способ передачи данных при встряхивании, способ инициирования по ключу, способ голосового запуска и способ скольжения вдоль дорожки.

[0110] В способе предварительно заданной инструкции получения данных в этой реализации настоящего изобретения, способы предварительно заданной инструкции получения данных, отличные от способа сканирования, должны быть заданы перед передачей данных. Например, способ передачи данных при встряхивании настраивается следующим образом: встряхивают дважды в одном направлении, встряхивают дважды влево и вправо и встряхивают трижды вверх и вниз. Способ инициирования по ключу включает в себя следующее: оконечное устройство проверки учетных данных отслеживает состояние инициирования по предварительно заданному ключу, и предварительно заданный ключ может быть физическим ключом или может быть виртуальным ключом. Когда клиентское программное обеспечение инициирует предварительно заданный ключ, оконечное устройство проверки учетных данных может получать двумерный штрих-код, отображаемый в клиентском программном обеспечении. Если клиентское программное обеспечение является клиентским программным обеспечением с сенсорным экраном, то после того, как оконечное устройство проверки учетных данных предварительно задает способ скольжения вдоль дорожки, оконечное устройство проверки учетных данных контролирует состояние скольжения сенсорного экрана в клиентском программном обеспечении, и когда пользователь клиентского программного обеспечения инициирует операцию скольжения на экране, получается двумерный штрих-код. Предварительно заданная инструкция получения данных описана выше, и тип предварительно заданной инструкции получения данных на практике не ограничен этой реализацией настоящего изобретения.

[0111] 402. Оконечное устройство проверки учетных данных проверяет период действия предварительно заданной информации безопасности и проверяет информацию подписи клиентского программного обеспечения и информацию подписи сервера.

[0112] Оконечное устройство проверки учетных данных анализирует полученный двумерный штрих-код, получает предварительно заданную информацию безопасности

и электронные учетные данные, которые включены в двумерный штрих-код, и проверяет период действия предварительно заданной информации безопасности и достоверность срока действия услуги в электронных учетных данных. Например, предположим, что предварительно заданная информация безопасности является текущим системным временем клиентского программного обеспечения, предварительно заданная информация безопасности составляет 10/21, а период действия предварительно заданной информации безопасности составляет 60 с. Оконечное устройство проверки учетных данных получает разницу во времени между текущим системным временем и предварительно заданной информацией безопасности и определяет, превышает ли период действия 60 с. Если определено, что период действия больше 60 с, оконечное устройство проверки учетных данных определяет, что двумерный штрих-код является недействительным. Предшествующее описание является примером. Кроме того, период действия предварительно заданной информации безопасности может быть установлен на две минуты и т.д. Период действия предварительно заданной информации безопасности не ограничен в этой реализации настоящего изобретения.

[0113] Для реализаций оконечного устройства проверки учетных данных, чтобы проверять информацию подписи клиентского программного обеспечения и информацию подписи сервера, ссылки могут быть сделаны к способу, показанному на фиг. 5. Подробности опущены для простоты в этом осуществлении настоящего изобретения.

[0114] 403. Если проверки каждой из предварительно заданной информации безопасности, информации подписи клиентского программного обеспечения и информации подписи сервера прошли успешно, получается срок действия услуги, включенной в электронные учетные данные для проверки.

[0115] Для проверки срока действия услуги могут быть сделаны ссылки на соответствующие описания в предыдущих реализациях. Подробности опущены для простоты в этом осуществлении настоящего изобретения.

[0116] 404. Если проверка срока действия услуги, включенного в электронные учетные данные, прошла успешно, определяется, что проверка электронных учетных данных прошла успешно.

[0117] Согласно способу обработки двумерных штрих-кодов, представленному в этом варианте осуществления настоящего изобретения, после приема запроса на получение электронных учетных данных, отправленного клиентским программным обеспечением, сервер подписывает электронные учетные данные и общедоступный ключ пользователя клиентского программного обеспечения с помощью секретного ключа сервера, чтобы получать информацию подписи сервера, и передает информацию подписи сервера и электронные учетные данные клиентскому программному обеспечению. Клиентское программное обеспечение принимает информацию подписи сервера и электронные учетные данные, которые отправляются сервером, проверяет информацию подписи сервера, после того как проверка информации подписи прошла успешно, подписывает электронные учетные данные и формирует двумерный штрих-код на основе предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя. После получения двумерного штрих-кода, оконечное устройство проверки учетных данных может проверять информацию подписи сервера, информацию подписи клиентского программного обеспечения и предварительно определенную информацию безопасности в двумерном штрих-коде, чтобы определять, были ли подделаны электронные учетные данные в процессе передачи, чтобы обеспечить безопасность электронных учетных

данных в процессе использования.

[0118] Кроме того, в качестве расширения способа, показанного на фиг. 6, в этой реализации настоящего изобретения все этапы способов выполняются на основе электронных учетных данных, формируемых оконечным устройством проверки учетных данных. Следовательно, в этой реализации настоящего изобретения до получения двумерного штрих-кода в клиентском программном обеспечении оконечное устройство проверки учетных данных формирует электронные учетные данные на основе идентификатора пользователя, и возможность формирования электронных учетных данных может включать в себя, но не ограничиваться, следующее содержимое. Например, после того, как пользователь покупает билет в билетном окне, билетная система формирует информацию электронных учетных данных в дополнении к формированию бумажных учетных данных и передает обратно информацию электронных учетных данных на сервер. Таким образом, сервер может отправлять электронные учетные данные клиентскому программному обеспечению. С другой стороны, после того, как пользователь покупает электронный билет на билетном сайте, электронные учетные данные, которые соответствуют электронному билету, формируются и затем отправляются на сервер. В этом варианте осуществления настоящего изобретения, не существует ограничений в отношении того, предоставляет ли оконечное устройство проверки учетных данных бумажный билет после формирования электронных учетных данных. В этом варианте осуществления настоящего изобретения электронные учетные данные предназначены для предотвращения сложных пост-регистрационных операций для бумажных учетных данных после того, как бумажные учетные данные потеряны или повреждены. Кроме того, безопасность электронных учетных данных может быть обеспечена, если оконечное устройство проверки учетных данных получает электронные учетные данные, которые внесены в динамический двумерный штрих-код.

[0119] После того как оконечное устройство проверки учетных данных сформирует электронные учетные данные, соответствующие электронные учетные данные могут быть синхронизированы с сервером на основе идентификационной информации пользователя, так что клиентское программное обеспечение может получать электронные учетные данные с сервера. В другом варианте осуществления настоящего изобретения, после приема информации запроса на получение электронных учетных данных, отправленного сервером, оконечного устройство проверки учетных данных отправляет электронные учетные данные на сервер, причем информация запроса на получение электронных учетных данных включает в себя идентификатор пользователя.

[0120] Кроме того, оконечное устройство проверки учетных данных может проверять информацию подписи клиентского программного обеспечения и информацию подписи сервера следующим способом и т.д. Например, оконечное устройство проверки учетных данных получает общедоступный ключ пользователя, включенный в двумерный штрих-код, и проверяет информацию подписи клиентского программного обеспечения на основе общедоступного ключа пользователя и электронных учетных данных. Оконечное устройство проверки учетных данных принимает и хранит общедоступный ключ сервера, соответствующий секретному ключу сервера, и распространяемый сервером; и проверяет информацию подписи сервера на основе общедоступного ключа сервера и электронных учетных данных.

[0121] Кроме того, в некоторых сценариях применения с относительно высокими требованиями к безопасности клиентское программное обеспечение использует информацию идентификатора пользователя в качестве информации атрибута

сформированного двумерного штрих-кода, так что оконечное устройство проверки учетных данных аутентифицирует информацию идентификации пользователя. Например, клиентское программное обеспечение использует удостоверение личности пользователя в качестве информации атрибута сформированного двумерного штрих-кода. Оконечное устройство проверки учетных данных анализирует двумерный штрих-код, получает идентификатор пользователя, включенный в оконечное устройство проверки учетных данных, и проверяет идентификатор пользователя. Если оконечное устройство проверки учетных данных определяет, что проверка по идентификатору пользователя прошла успешно, то оконечное устройство проверки учетных данных определяет, что проверка по электронным учетным данным прошла успешно. Например, когда электронные учетные данные в двумерном штрих-коде являются билетом на поезд, когда пользователь использует электронный билет на поезд для прохождения через турникет станции, то удостоверение личности пользователя может быть проверено в то же самое время, чтобы завершать проверку электронных учетных данных.

[0122] Кроме того, когда оконечное устройство проверки учетных данных проверяет содержимое двумерного штрих-кода, независимо от объема содержимого, включенной в двумерный штрих-код, до тех пор, пока содержимое, включенное в двумерный штрих-код, успешно проверяется оконечным устройством проверки учетных данных, это показывает, что проверка электронных учетных данных прошла успешно. Если один элемент или некоторые элементы, включенные в двумерный штрих-код, не прошли проверку, это означает, что проверка электронных учетных данных не пройдена. Например, предположим, что, когда двумерный штрих-код включает в себя предварительно заданную информацию безопасности, информацию подписи клиентского программного обеспечения, информацию подписи сервера и идентификатор пользователя, можно определить, что электронные учетные данные успешно проверены только после того, как проверка каждой из предварительно заданной информация безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера и идентификатора пользователя прошла успешно.

[0123] Как описано выше, оконечное устройство проверки учетных данных проверяет электронные учетные данные, которые переносятся в двумерном штрих-коде, и из этого процесса видно удобство и безопасность электронных учетных данных в повседневной работе и жизни. Предыдущее описание описывается с помощью примера, что клиентское программное обеспечение включает в себя один тип электронных учетных данных. На практике клиентское программное обеспечение может включать в себя множество типов электронных учетных данных. Электронные учетные данные могут быть отдельно записаны в различных динамических двумерных штрих-кодах или могут быть записаны в одном и том же двумерном штрих-коде. Реализации не ограничены в этом осуществлении настоящего изобретения. Электронные учетные данные могут заменять информацию учетных данных объекта в существующей технологии, предотвращая утечку информации учетных данных объекта и облегчая громоздкие этапы отмены регистрации или пост-регистрации, когда учетные данные объекта теряются. Согласно способу в этом варианте осуществления настоящего изобретения, пользователю только нужно при выходе носить с собой одно терминальное устройство (мобильный телефон), с установленным клиентским программным обеспечением, и не нужно носить с собой какой-либо другой объект учетных данных.

[0124] Например, пользователь А несет только один мобильный телефон, с установленный клиентским программным обеспечением, и едет на автобусе от дома до компании в 8:00 утра. Пользователь может перемещаться беспрепятственно с

двумерным штрих-кодом электронных учетных данных на автобус в клиентском программном обеспечении. После прибытия, пользователь может войти в компанию с контролем доступа по электронным учетным данным и может отмечать время прихода на работу с помощью электронных учетных данных. В 11:00 утра, пользователь А должен пойти в банк для получения банковских услуги, и электронное удостоверение личности и электронная банковская карта могут быть использованы для получения услуг. В 17:00, пользователь А должен ехать к вокзалу для отправления в командировку. Когда пользователь А проходит через турникет, проверка настоящего имени может быть выполнена с использованием электронного удостоверения личности и электронного билета на поезд. После успешной проверки пользователь может сесть на поезд. Предыдущий безопасный способ обработки двумерных штрих-кодов используется после проверки электронных учетных данных. Предыдущий пример предназначен для иллюстрации удобства и безопасности, привнесенных электронными учетными данными в жизнь и работу, и не предназначен для ограничения на конкретный сценарии применения электронных учетных данных.

[0125] В предыдущих реализациях процессы, в которых сервер, клиентское программное обеспечение и оконечное устройство проверки учетных данных обрабатывают двумерные штрих-коды, подробно описаны отдельно. Однако на практике сервер, клиентское программное обеспечение и оконечное устройство проверки учетных данных незаменимы при проверке двумерного штрих-кода. В следующих реализациях сервер, клиентское программное обеспечение и оконечное устройство проверки учетных данных обобщены и описаны. Как показано на фиг. 7, способ включает в себя следующие этапы.

[0126] 501. Оконечное устройство проверки учетных данных формирует электронные учетные данные на основе идентификатора пользователя, и синхронизирует соответствующее электронные учетные данные с сервером на основе идентификатора пользователя, так что сервер отправляет электронные учетные данные в клиентское программное обеспечение.

[0127] 502. Клиентское программное обеспечение отправляет запрос на получение электронных учетных данных на сервер, причем запрос на получение электронных учетных данных включает в себя идентификатор пользователя и срок действия услуги.

[0128] 503. Сервер принимает запрос на получение электронных учетных данных, отправленный клиентским программным обеспечением, анализирует запрос на получение электронных учетных данных и получает срок действия услуги, включенный в запрос на получение электронных учетных данных.

[0129] 504. Сервер проверяет, соответствует ли срок действия услуги спецификации услуги.

[0130] Если срок действия услуги соответствует спецификации услуги, выполняется этап 505. Если срок действия услуги не соответствует спецификации услуги, запрос на получение электронных учетных данных игнорируется.

[0131] 505. Получение электронных учетных данных, которые соответствуют идентификатору пользователя, и шифрование электронных учетных данных.

[0132] Информация запроса на получение электронных учетных данных может быть дополнительно направлена в оконечное устройство проверки учетных данных, на основе идентификатора пользователя, чтобы получать электронные учетные данные.

[0133] 506. Сервер подписывает общедоступный ключ пользователя клиентского программного обеспечения и электронные учетные данные, используя секретный ключ сервера, для получения информации подписи сервера и отправляет информацию подписи

сервера и электронные учетные данные в клиентское программное обеспечение.

[0134] 507. Сервер распространяет общедоступный ключ, соответствующий секретному ключу сервера, так что клиентское программное обеспечение и оконечное устройство проверки учетных данных проверяют информацию подписи на основе общедоступного ключа сервера.

[0135] 508. Клиентское программное обеспечение принимает и хранит общедоступный ключ, распространяемый сервером.

[0136] 509. Клиентское программное обеспечение принимает информацию подписи сервера и электронные учетные данные, отправленные сервером.

[0137] 510. Клиентское программное обеспечение проверяет информацию подписи сервера на основе общедоступного ключа, распространенного сервером, чтобы получать электронные учетные данные.

[0138] Если проверка информации подписи сервера прошла успешно, выполняется этап 511. Если проверка информации подписи сервера не прошла успешно, электронные учетные данные, предоставляемые сервером, не могут быть получены.

[0139] 511. Клиентское программное обеспечение подписывает электронные учетные данные с помощью ключа пользователя, чтобы получать информацию подписи клиентского программного обеспечения, и формирует двумерный штрих-код на основе предварительно заданной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя.

[0140] 512. Оконечное устройство проверки учетных данных получает двумерный штрих-код в клиентском программном обеспечении, проверяет срок действия предварительно заданной информации безопасности и проверяет информацию подписи клиентского программного обеспечения и информацию подписи сервера.

[0141] 513. Если проверка каждой из предварительно заданной информации безопасности, информации подписи клиентского программного обеспечения и информации подписи сервера прошла успешно, получается срок действия услуги, включенный в электронные учетные данные для проверки; и если проверка срока действия услуги, включенного в электронные учетные данные, прошла успешно, определяется, что проверка электронных учетных данных прошла успешно.

[0142] Стоит отметить, что для подробного описания этапов 501-513 могут быть сделаны ссылки на предыдущие связанные описания. Подробности опущены для простоты в этом осуществлении настоящего изобретения.

[0143] Кроме того, как реализация способа, показанного на фиг. 1, так и другая реализация настоящего изобретения дополнительно предоставляет сервер. Эта реализация оборудования соответствует предыдущему способу реализации. Для простоты чтения подробности из предыдущей реализации способа в этой реализации оборудования опущены. Однако, должно быть понятно, что оборудование в этой реализации может соответственно реализовывать все содержимое из предыдущей реализации способа.

[0144] Кроме того, реализация настоящего изобретения предоставляет сервер. Как показано на фиг. 8, оборудование включает в себя следующее: приемный блок 61, сконфигурированный, чтобы принимать запрос на получение электронных учетных данных, отправленный клиентским программным обеспечением, причем запрос на получение электронных учетных данных включает в себя идентификатор пользователя; первый блок 62 получения, сконфигурированный для получения электронных учетных данных, которые соответствуют идентификатору пользователя, принятому приемным

блоком; блок 63 подписи, сконфигурированный для подписи электронных учетных данных и общедоступного ключа пользователя клиентского программного обеспечения с помощью секретного ключа сервера для получения информации подписи сервера; и блок 64 отправки, сконфигурированный, чтобы отправлять информацию подписи сервера, полученную с помощью блока 63 подписи, и электронные учетные данные, полученные первым блоком получения, клиентскому программному обеспечению, так что клиентское программное обеспечение проверяет информацию подписи сервера в течение срока действия ключа пользователя и формирует двумерный штрих-код на основе электронных учетных данных, таким образом, чтобы оконечное устройство проверки учетных данных проверяло электронные учетные данные, включенные в двумерный штрих-код, причем оконечное устройство проверки учетных данных сконфигурировано для формирования электронных учетных данных на основе идентификатора пользователя.

[0145] Кроме того, как показано на фиг. 9, блок 63 подписи включает в себя следующее: модуль 631 выделения, сконфигурированный, чтобы выделять ключ подписи пользователя электронным учетным данным; первый модуль 632 подписи, сконфигурированный, чтобы подписывать с помощью секретного ключа сервера электронные учетные данные и первый общедоступный ключ пользователя, выделенный модулем выделения, причем выделенный ключ подписи пользователя включает в себя первый общедоступный ключ пользователя; модуль 633 получения, сконфигурированный, чтобы получать второй общедоступный ключ пользователя, отправленный клиентским программным обеспечением; и второй модуль 634 подписи, сконфигурированный, чтобы подписывать с помощью секретного ключа сервера электронные учетные данные и второй общедоступный ключ пользователя, полученные модулем получения.

[0146] Кроме того, если первый общедоступный ключ пользователя подписан с использованием секретного ключа сервера, блок 64 отправки дополнительно сконфигурирован, чтобы отправлять выделенный ключ подписи пользователя, информацию подписи сервера и электронные учетные данные клиентскому программному обеспечению.

[0147] Кроме того, как показано на фиг. 9, сервер дополнительно включает в себя следующее: блок 65 анализа, сконфигурированный, чтобы: перед тем как первый блок 62 получения получает электронные учетные данные, которые соответствуют идентификатору пользователя, анализировать запрос на получение электронных учетных данных; второй блок 66 получения, сконфигурирован, чтобы: после того, как блок 65 анализа анализирует запрос на получение электронных учетных данных, получать срок действия услуги, включенный в запрос на получение электронных учетных данных; и блок 67 проверки, сконфигурированный, чтобы проверять, удовлетворяет ли срок действия услуги, полученный с помощью второго блока 66 получения требованию спецификации услуги, причем первый блок 62 получения дополнительно сконфигурирован, чтобы: когда блок 67 проверки проверяет, что срок действия услуги соответствует спецификации услуги, получать электронные учетные данные, которые соответствуют идентификатору пользователя.

[0148] Кроме того, как показано на фиг. 9, первый блок 62 получения включает в себя следующее: приемный модуль 621, сконфигурированный, чтобы: после того, как оконечное устройство проверки учетных данных формирует электронные учетные данные на основе идентификатора пользователя, принимать электронные учетные данные, синхронизированные с оконечным устройством проверки учетных данных; и

модуль 622 обработки, сконфигурированный, чтобы отправлять информацию запроса для получения электронных учетных данных для оконечного устройства проверки учетных данных на основе идентификатора пользователя, чтобы получать электронные учетные данные.

[0149] Кроме того, ключ подписи пользователя является асимметричным ключом.

[0150] Кроме того, как показано на фиг. 9, сервер дополнительно включает в себя следующее: блок 68 распространения, сконфигурированный, чтобы распространять общедоступный ключ, соответствующий секретному ключу сервера, так что клиентское программное обеспечение и оконечное устройство проверки учетных данных проверяют информацию подписи на основе общедоступного ключа сервера.

[0151] Реализация настоящего изобретения дополнительно предоставляет клиентское программное обеспечение. Как показано на фиг. 10, клиентское программное обеспечение включает в себя следующее: первый приемный блок 71, сконфигурированный для приема информации подписи сервера и электронных учетных данных, которые отправляются сервером, где информация подписи сервера получается сервером путем подписания электронных учетных данных и общедоступного ключа пользователя клиентского программного обеспечения с помощью секретного ключа сервера; блок 72 проверки подписи, сконфигурированный для проверки информации подписи сервера, чтобы получать электронные учетные данные; блок 73 получения, сконфигурированный для получения ключа пользователя, который соответствует общедоступному ключу пользователя; блок 74 подписи, сконфигурированный для подписания электронных учетных данных с помощью ключа пользователя, полученного блоком 73 получения для получения информации подписи клиентского программного обеспечения; и блок 75 формирования, сконфигурированный для формирования двумерного штрих-кода на основе предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя, так что оконечное устройство проверки учетных данных проверяет электронные учетные данные, включенные в двумерный штрих-код, на основе предварительно определенной информации безопасности и общедоступного ключа пользователя, причем предварительно определенная информация безопасности имеет срок действия, и оконечное устройство проверки учетных данных сконфигурировано для формирования электронных учетных данных на основе идентификатора пользователя.

[0152] Кроме того, как показано на фиг. 11, клиентское программное обеспечение дополнительно включает в себя следующее: второй приемный блок 76, сконфигурированный, чтобы: до получения ключа пользователя, который соответствует общедоступному ключу пользователя, принимать ключ подписи пользователя, выделенный для электронных учетных данных и отправленный сервером.

[0153] Блок 73 получения дополнительно сконфигурирован, чтобы получать первый ключ пользователя, включенный в ключ подписи пользователя, который выделен сервером для электронных учетных данных и который принимается вторым приемным блоком.

[0154] Блок 73 получения дополнительно сконфигурирован, чтобы получать второй ключ пользователя, сформированный клиентским программным обеспечением и соответствующий общедоступному ключу пользователя.

[0155] Кроме того, как показано на фиг. 11, блок 74 подписи включает в себя следующее: первый модуль 741 подписи, сконфигурированный, чтобы подписывать

электронные учетные данные с использованием первого ключа пользователя; и второй модуль 742 подписи, сконфигурированный, чтобы подписывать электронные учетные данные с использованием второго ключа пользователя.

[0156] Кроме того, как показано на фиг. 11, блок 72 проверки подписи включает в себя следующее: приемный модуль 721, сконфигурированный, чтобы принимать общедоступный ключ сервера, распространяемый сервером; модуль 722 хранения, сконфигурированный, чтобы хранить общедоступный ключ сервера, принятый приемным модулем; и модуль 723 проверки первой подписи, сконфигурированный, чтобы проверять информацию подписи сервера на основе общедоступного ключа сервера, хранящегося в модуле хранения, общедоступного ключа клиентского программного обеспечения и электронных учетных данных.

[0157] Кроме того, общедоступный ключ пользователя и ключ пользователя являются асимметричными ключами.

[0158] Кроме того, как показано на фиг. 11, блок 75 формирования включает в себя следующее: модуль 751 настройки, сконфигурированный, чтобы устанавливать период действия предварительно заданной информации безопасности; и модуль 752 формирования, сконфигурированный, чтобы формировать двухмерный штрих-код на основе предварительно заданной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных, общедоступного ключа пользователя, периода действия предварительно заданной информации безопасности и идентификатора пользователя.

[0159] Реализация настоящего изобретения дополнительно предоставляет оконечное устройство проверки учетных данных. Как показано на фиг. 12, оконечное устройство проверки учетных данных включает в себя следующее: первый блок 81 получения, сконфигурированный для получения двумерного штрих-кода в клиентском программном обеспечении, где двумерный штрих-код формируется клиентским программным обеспечением на основе предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя, информация подписи клиентского программного обеспечения получается с помощью клиентского программного обеспечения путем подписания электронных учетных данных, и информация подписи сервера получается сервером путем подписания электронных учетных данных и общедоступного ключа пользователя; первый блок 82 проверки, сконфигурированный для проверки срока действия предварительно определенной информации безопасности, полученной первым блоком получения; второй блок 83 проверки, сконфигурированный для проверки информации подписи клиентского программного обеспечения и информации подписи сервера; третий блок 84 проверки, сконфигурированный для получения срока действия услуги, включенной в электронные учетные данные для проверки, когда проверка первого блока проверки по предварительно определенной информации безопасности прошла успешно, проверка второго блока проверки по каждой информации подписи клиентского программного обеспечения и информации подписи сервере прошла успешно; и блок 85 определения, сконфигурированный для определения того, что проверка электронных ученых данных завершается успешно, когда проверка третьего блока проверки на срок действия услуги, включенный в электронные учетные данные, прошла успешно.

[0160] Кроме того, как показано на фиг. 13, оконечное устройство проверки учетных данных дополнительно включает в себя следующее: блок 86 формирования, сконфигурированный, чтобы формировать электронные учетные данные на основе

идентификатора пользователя, перед тем, как первый блок 81 получения получает двумерный штрих-код в клиентском программном обеспечении; блок 87 синхронизации, сконфигурированный, чтобы синхронизировать соответствующее электронные учетные данные с сервером на основе идентификатора пользователя, так что сервер отправляет электронные учетные данные клиентскому программному обеспечению; приемный блок 88, сконфигурированный, чтобы принимать информацию запроса на получение электронных учетных данных, отправленных сервером; и блок 89 отправки, сконфигурированный, чтобы отправлять электронные учетные данные на сервер, причем информация запроса на получение электронных учетных данных включает в себя идентификатор пользователя.

[0161] Кроме того, как показано на фиг. 13, второй блок 83 проверки включает в себя следующее: модуль 831 получения, сконфигурированный, чтобы получать общедоступный ключ пользователя, включенный в двумерный штрих-код; первый модуль 832 проверки подписи, сконфигурированный, чтобы проверять информацию подписи клиентского программного обеспечения на основе общедоступного ключа пользователя, полученного с помощью модуля получения и электронных учетных данных; приемный модуль 833, сконфигурированный, чтобы принимать общедоступный ключ сервера, соответствующий секретному ключу сервера и распространенный сервером; модуль 834 хранения, сконфигурированный, чтобы хранить общедоступный ключа сервера, принятый приемным модулем; и второй модуль 835 проверки, сконфигурированный, чтобы проверять информацию подписи сервера на основе общедоступного ключа сервера, сохраненного в модуле хранения, общедоступного ключа клиентского программного обеспечения и электронных учетных данных.

[0162] Кроме того, как показано на фиг. 13, оконечное устройство проверки учетных данных дополнительно включает в себя следующее: второй блок 810 получения, сконфигурированный, чтобы: до того, как блок 85 определения определяет, что проверка электронных учетных данных прошла успешно, получать идентификатор пользователя, включенный в двумерный штрих-код; и четвертый блок 811 проверки, сконфигурированный, чтобы проверять идентификатор пользователя, полученный с помощью второго блока 810 получения.

[0163] Блок 85 определения дополнительно сконфигурирован, чтобы: когда четвертый блок 811 проверки определяет, что проверка идентификатора пользователя прошла успешно, определять, что проверка электронных учетных данных прошла успешно.

[0164] Кроме того, как показано на фиг. 14, реализация настоящего изобретения дополнительно предоставляет систему для обработки двумерных штрих-кодов, и система включает в себя следующее: клиентское программное обеспечение 91, сконфигурированное, чтобы отправлять запрос на получение электронных учетных данных на сервер 92, причем запрос на получение электронных учетных данных включает в себя идентификатор пользователя; сервер 92, сконфигурированный, чтобы принимать запрос на получение электронных учетных данных, отправленный клиентским программным обеспечением 91, и получать электронные учетные данные от оконечного устройства 93 проверки учетных данных на основе идентификатора пользователя; и оконечное устройство 93 проверки учетных данных, сконфигурированное, чтобы принимать и отвечать на запрос информации для получения электронных учетных данных, отправленный сервером 92, и отправлять электронные учетные данные серверу 92.

[0165] Сервер 92 дополнительно сконфигурирован, чтобы принимать электронные учетные данные, отправленные оконечным устройством 93 проверки учетных данных,

подписывать электронные учетные данные и общедоступный ключ пользователя клиентского программного обеспечения 91, чтобы получать информацию подписи сервера 92, и отправлять информацию подписи сервера 92 и электронные учетные данные клиентскому программному обеспечению 91.

[0166] Клиентское программное обеспечение 91 сконфигурировано, чтобы принимать информацию подписи сервера 92 и электронные учетные данные, которые отправлены сервером 92, проверять информацию подписи сервера 92, чтобы получать электронные учетные данные, получать ключ пользователя, соответствующий общедоступному ключу пользователя, подписывать электронные учетные данные с помощью ключа пользователя, чтобы получать информацию подписи клиентского программного обеспечения 91, и формировать двумерный штрих-код на основе предварительно заданной информации безопасности, информации подписи клиентского программного обеспечения 91, информации подписи сервера 92, электронных учетных данных и общедоступного ключа пользователя.

[0167] Оконечное устройство 93 проверки учетных данных сконфигурировано, чтобы получать двумерный штрих-код в клиентском программном обеспечении 91, проверять период действия предварительно заданной информации безопасности и проверять информацию подписи клиентского программного обеспечения 91 и информацию подписи сервера 92; и если проверка каждой из предварительно заданной информации безопасности, информации подписи клиентского программного обеспечения 91 и информации подписи сервера 92 прошла успешно, получать срок действия услуги, включенный в электронные учетные данные для проверки и, если проверка срока действия услуги, включенного в электронные учетные данные прошла успешно, определять, что проверка электронных учетных данных прошла успешно.

[0168] Согласно серверу, клиентскому программному обеспечению, оконечному устройству проверки учетных данных, системе для обработки двумерных штрих-кодов, предусмотренных в настоящем изобретении, после приема запроса на получение электронных учетных данных, отправленного клиентским программным обеспечением, сервер подписывает электронные учетные данные и общедоступный ключ пользователя клиентского программного обеспечения с помощью секретного ключа сервера, чтобы получать информацию подписи сервера, и отправляет информацию подписи сервера и электронные учетные данные клиентскому программному обеспечению. Клиентское программное обеспечение принимает информацию подписи сервера и электронные учетные данные, которые отправляются сервером, проверяет информацию подписи сервера, после того как проверка информации подписи прошла успешно, подписывает электронные учетные данные и формирует двумерный штрих-код на основе предварительно определенной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных и общедоступного ключа пользователя. После получения двумерного штрих-кода, оконечное устройство проверки учетных данных может проверять информацию подписи сервера, информацию подписи клиентского программного обеспечения и предварительно определенную информацию безопасности в двумерном штрих-коде, чтобы определять, были ли подделаны электронные учетные данные в процессе передачи, чтобы обеспечить безопасность электронных учетных данных в процессе использования.

[0169] В предыдущих реализациях описание каждой реализации имеет соответствующие акценты. Для части, не описанной подробно в реализации, могут быть сделаны ссылки на соответствующие описания в других реализациях.

[0170] Понятно, что на связанные признаки в предыдущем способе и оборудовании можно взаимно ссылаться. Кроме того, "первый", "второй" и т.д.

в предыдущей реализации используются для различия между реализациями и не представляют преимущества и недостатки каждой реализации.

[0171] Специалист в данной области может четко понимать, что для удобства и краткости описания, для конкретного рабочего процесса системы, оборудования и блока, описанного выше, могут быть сделаны ссылки на соответствующий процесс в предыдущих реализациях способа, и подробности опущены для простоты при реализации настоящего изобретения.

[0172] Алгоритм и отображение, представленные здесь, по сути, не связаны с каким-либо конкретным компьютером, виртуальной системой или другими устройствами. Различные системы общего назначения также могут использоваться вместе с инструкциями, основанными здесь. На основании приведенного выше описания, структура, необходимая для построения такой системы, очевидна. Кроме того, настоящее изобретение не относится к какому-либо конкретному языку программирования. Следует понимать, что содержимое настоящего изобретения, описанное здесь, может быть реализовано с помощью различных языков программирования, и предыдущее описание подробным языком используется для раскрытия лучшего осуществления настоящего изобретения.

[0173] Большое количество деталей предоставлено в сущности. Однако может быть понятно, что реализации настоящего изобретения могут быть осуществлены на практике без этих деталей. В некоторых случаях общеизвестные способы, структуры и технологии не показаны подробно, чтобы не размывать понимание настоящего описания.

[0174] Аналогичным образом, следует понимать, что для упрощения настоящего описания и для помощи в понимании одного или нескольких из различных аспектов изобретения, признаки настоящего изобретения иногда группируются в одной реализации, чертеже или описании настоящего изобретения. Однако раскрытый способ не следует интерпретировать как отражающий следующее намерение: так, заявленное раскрытие требует большего количества признаков, чем признаки, указанные в каждой формуле изобретения. Более точно, как это отражено в приведенных ниже пунктах формулы изобретения, аспектов изобретения меньше, чем всех признаков одной реализации, описанной ранее. Следовательно, пункты формулы изобретения, которые следуют за подробной реализацией, определенно включают в себя подробную реализацию. Каждый пункт формулы изобретения служит в качестве отдельной реализации настоящего изобретения.

[0175] Специалист в данной области техники может понимать, что модули в устройствах в реализациях могут быть адаптивно изменены и размещены в одном или нескольких устройствах, различных от реализаций. Модули, или блоки, или компоненты в реализациях могут быть объединены в один модуль, или блок, или компонент, и дополнительно могут быть разделены на множество подмодулей, или подблоков, или субкомпонентов. За исключением случаев того, что по крайней мере некоторые из этих признаков, и/или процессов, или блоков являются взаимоисключающими, все описанные признаки и все процессы или блоки любого способа или устройства, которые раскрыты в таком способе в описании (в том числе в прилагаемой формуле изобретения, реферате и сопроводительных чертежах), можно комбинировать в любом режиме комбинирования. Если иное не указано, каждый признак, раскрытый в данном описании (включая прилагаемую формулу изобретения, реферат и сопроводительные чертежи), может быть заменен альтернативной функцией, которая служит таким же,

эквивалентным или аналогичным целям.

[0176] Кроме того, специалисты в данной области техники могут понимать, что, хотя некоторые реализации, описанные здесь, включают в себя некоторые признаки, включенные в другую реализацию вместо того, чтобы включать в себя другие признаки, комбинация признаков различных реализаций означает попадание под объем настоящего изобретения и формирование различных реализаций. Например, в следующей формуле изобретения любая из рассмотренных реализаций может использоваться в любом комбинированном режиме.

[0177] Реализации различных частей в настоящем изобретении могут быть реализованы с помощью аппаратных или программных модулей, работающих на одном или нескольких процессорах, или их комбинации. Специалисту в данной области техники должно быть понятно, что микропроцессор или цифровой сигнальный процессор (DSP) могут быть использованы на практике для реализации некоторых или всех функций некоторых или всех компонентов раскрытия (например, оборудование для обработки двумерного штрих-кода), основанных на реализации настоящего изобретения. Настоящее изобретение также может быть реализовано как программа оборудования или устройства (например, компьютерная программа и компьютерный программный продукт) для выполнения части или всех способов, описанных здесь. Такая программа для реализации настоящего изобретения может быть сохранена на машиночитаемом носителе или может иметь форму одного или нескольких сигналов. Такой сигнал можно загрузить с интернет-сайта, или представлен в сигнале несущей, или представлен в любой другой форме.

[0178] Стоит отметить, что предыдущие реализации предназначены для описания настоящего изобретения, а не ограничивают объем настоящего изобретения, и специалисты в данной области техники могут разработать альтернативную реализацию без отступления от сущности и объема прилагаемой формулы изобретения. В формуле изобретения любой символ ссылки, расположенный в скобках, не должен конструироваться как ограничение формулы изобретения. Слово "включать" не исключает существования элементов или этапов, не указанных в формуле изобретения. Слово "один" перед элементом или упоминание элемента в единственном числе не исключает присутствия множества таких элементов. Настоящее изобретение может быть реализовано с помощью аппаратных средств, включающих в себя несколько различных элементов на компьютере, который соответствующим образом запрограммирован. В пунктах формулы изобретения, перечисляющих несколько устройств, несколько из этих устройств могут быть воплощены с использованием одного и того же элемента аппаратного обеспечения. Использование слов "первый", "второй" и "третий" не указывает на какую-либо последовательность. Эти слова можно интерпретировать как имена.

(57) Формула изобретения

1. Способ обработки двумерных штрих-кодов, содержащий этапы, на которых:

принимают посредством сервера запрос на получение электронных учетных данных, отправленный клиентским программным обеспечением, причем запрос на получение электронных учетных данных содержит идентификатор пользователя;

получают посредством сервера электронные учетные данные, которые соответствуют идентификатору пользователя, причем электронные учетные данные формируются оконечным устройством проверки учетных данных на основе идентификатора пользователя;

посредством сервера подписывают электронные учетные данные и общедоступный ключ пользователя клиентского программного обеспечения с использованием секретного ключа сервера для получения информации подписи сервера и отправляют информацию подписи сервера и электронные учетные данные в клиентское программное обеспечение; и

посредством клиентского программного обеспечения проверяют информацию подписи сервера и формируют двумерный штрих-код на основе, по меньшей мере, электронных учетных данных с тем, чтобы оконечное устройство проверки учетных данных проверяло электронные учетные данные, содержащиеся в двумерном штрих-коде.

2. Способ по п. 1, в котором подписание электронных учетных данных с использованием секретного ключа сервера содержит этапы, на которых:

выделяют ключ подписи пользователя для электронных учетных данных и подписывают электронные учетные данные и первый общедоступный ключ пользователя с помощью секретного ключа сервера, причем выделенный ключ подписи пользователя содержит первый общедоступный ключ пользователя; или

получают второй общедоступный ключ пользователя, отправленный клиентским программным обеспечением, и подписывают электронные учетные данные и второй общедоступный ключ пользователя с помощью секретного ключа сервера.

3. Способ по п. 2, в котором ключ подписи пользователя является асимметричным ключом.

4. Способ по п. 2, в котором первый общедоступный ключ пользователя подписан с использованием секретного ключа сервера, при этом отправка информации подписи сервера и электронных учетных данных в клиентское программное обеспечение содержит этап, на котором отправляют выделенный ключ подписи пользователя, информацию подписи сервера и электронные учетные данные в клиентское программное обеспечение.

5. Способ по любому из пп. 1-4, при этом перед получением электронных учетных данных, которые соответствуют идентификатору пользователя, способ дополнительно содержит этапы, на которых:

анализируют запрос на получение электронных учетных данных и получают срок действия услуги, указанный в запросе на получение электронных учетных данных; и

проверяют, соответствует ли срок действия услуги спецификации услуги.

6. Способ по п. 5, в котором получение электронных учетных данных, которые соответствуют идентификатору пользователя, содержит этап, на котором: если срок действия услуги соответствует спецификации услуги, получают электронные учетные данные, которые соответствуют идентификатору пользователя.

7. Способ по п. 6, в котором получение электронных учетных данных, которые соответствуют идентификатору пользователя, содержит этапы, на которых:

после того, как оконечное устройство проверки учетных данных формирует электронные учетные данные на основе идентификатора пользователя, принимают электронные учетные данные, синхронизированные оконечным устройством проверки учетных данных; или

отправляют информацию запроса на получение электронных учетных данных в оконечное устройство проверки учетных данных на основе идентификатора пользователя, чтобы получать электронные учетные данные.

8. Способ по п. 6, при этом способ дополнительно содержит этап, на котором распространяют общедоступный ключ, соответствующий секретному ключу сервера,

так что клиентское программное обеспечение и оконечное устройство проверки учетных данных проверяют информацию подписи на основе общедоступного ключа сервера.

9. Способ по п. 1, в котором двумерный штрих-код формируется путем выполнения операций, содержащих этапы, на которых:

устанавливают период действия предварительно заданной информации безопасности; и

формируют двумерный штрих-код на основе предварительно заданной информации безопасности, информации подписи клиентского программного обеспечения, информации подписи сервера, электронных учетных данных, общедоступного ключа пользователя, периода действия предварительно заданной информации безопасности и идентификатора пользователя.

10. Способ по п. 1, дополнительно содержащий этап, на котором синхронизируют электронные учетные данные с сервером на основе идентификатора пользователя, чтобы сервер отправлял электронные учетные данные в клиентское программное обеспечение.

11. Способ по п. 1, в котором период действия предварительно заданной информации безопасности основывается на типе электронных учетных данных.

12. Способ по п. 1, в котором электронные учетные данные содержат авиабилет, билет на автобус, билет на поезд, билет на концерт, банковскую карту, карту контроля доступа, входной билет в парк, удостоверение личности, купон на скидку, членский билет, водительские права, карту контроля доступа водительских прав или автобусную карту.

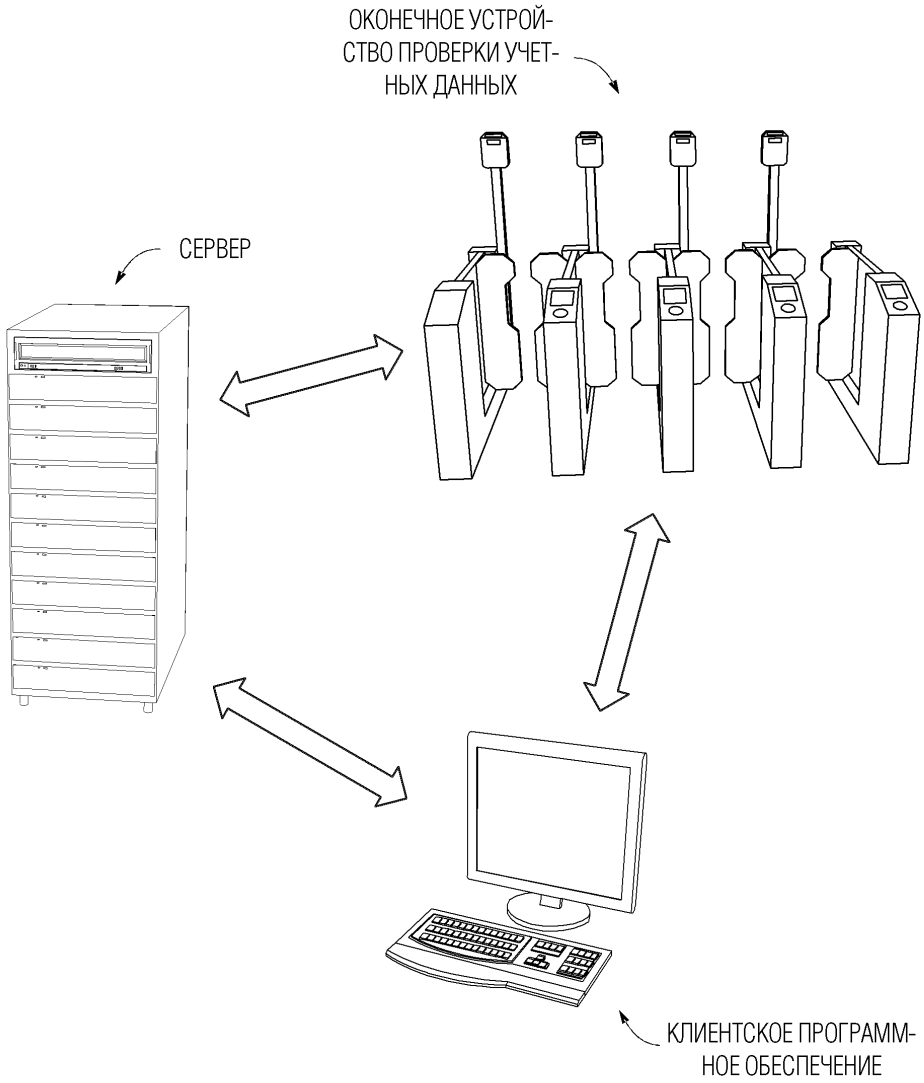
13. Способ по п. 1, в котором подписание электронных учетных данных и общедоступного ключа пользователя содержит этапы, на которых:

выполняют операцию хеширования общедоступного ключа пользователя и электронных учетных данных с использованием алгоритма хеширования для получения значения хеш-функции; и

подписывают значение хеш-функции с использованием секретного ключа сервера для получения информации подписи сервера.

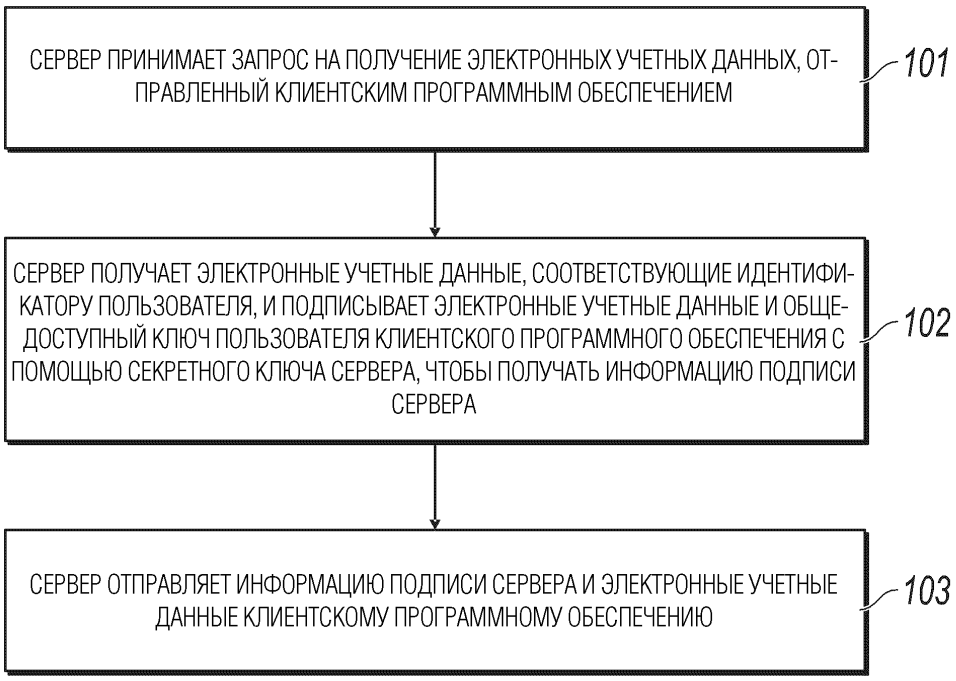
14. Система для обработки двумерных штрих-кодов, содержащая два или более вычислительных устройств, выполненных с возможностью осуществления связи друг с другом, причем каждое из вычислительных устройств содержит один или более процессоров и один или более машиночитаемых носителей, при этом на машиночитаемых носителях хранятся машиноисполняемые инструкции, которые при их исполнении процессорами предписывают вычислительным устройствам выполнять способ по любому из пп. 1-13.

1


ОКОНЕЧНОЕ УСТРОЙ-
СТВО ПРОВЕРКИ УЧЕТ-
НЫХ ДАННЫХ
СЕРВЕР
КЛИЕНТСКОЕ ПРОГРАММ-
НОЕ ОБЕСПЕЧЕНИЕ

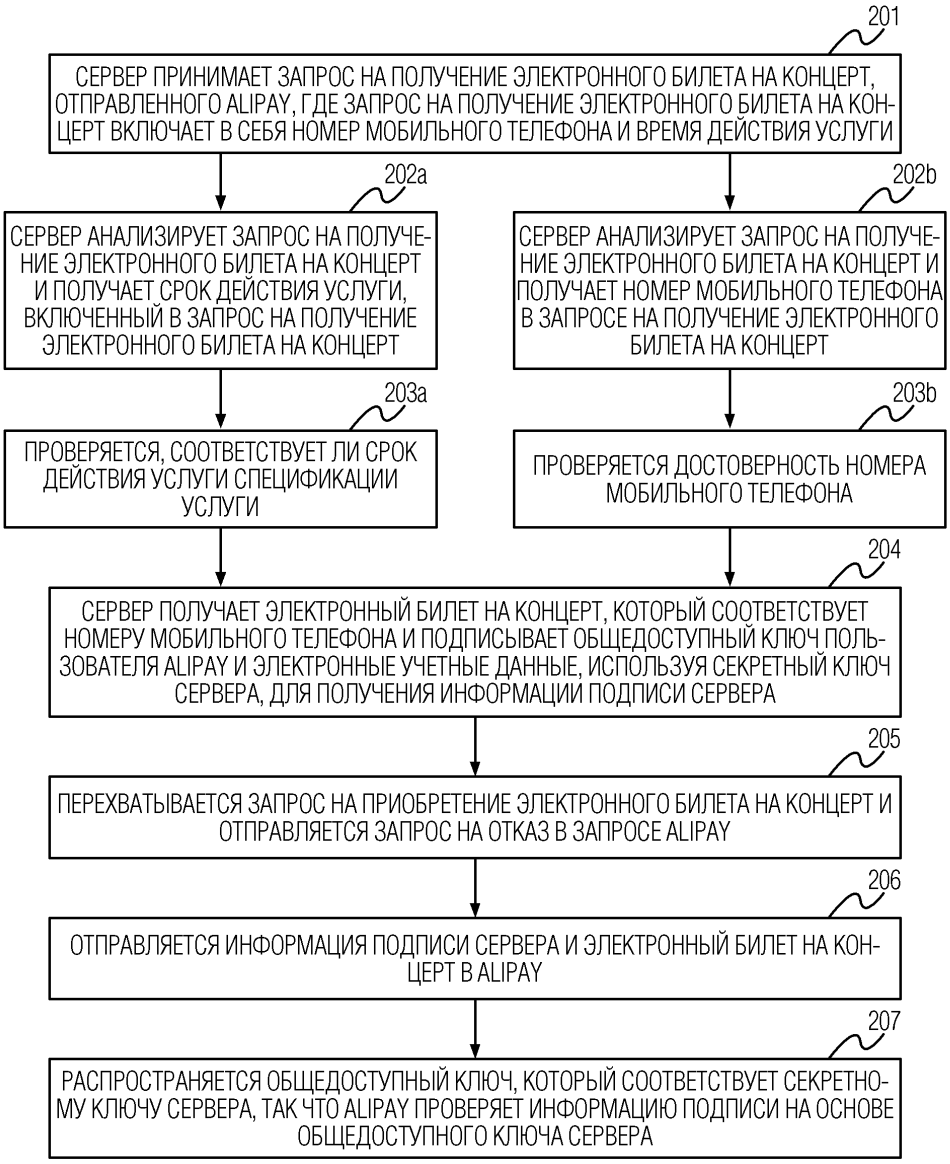
ФИГ. 1

2


СЕРВЕР ПРИНИМАЕТ ЗАПРОС НА ПОЛУЧЕНИЕ ЭЛЕКТРОННЫХ УЧЕТНЫХ ДАННЫХ, ОТПРАВЛЕННЫЙ КЛИЕНТСКИМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ
101
СЕРВЕР ПОЛУЧАЕТ ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ, СООТВЕТСТВУЮЩИЕ ИДЕНТИФИКАТОРУ ПОЛЬЗОВАТЕЛЯ, И ПОДПИСЫВАЕТ ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ И ОБЩЕДОСТУПНЫЙ КЛЮЧ ПОЛЬЗОВАТЕЛЯ КЛИЕНТСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ПОМОЩЬЮ СЕКРЕТНОГО КЛЮЧА СЕРВЕРА, ЧТОБЫ ПОЛУЧАТЬ ИНФОРМАЦИЮ ПОДПИСИ СЕРВЕРА
102
СЕРВЕР ОТПРАВЛЯЕТ ИНФОРМАЦИЮ ПОДПИСИ СЕРВЕРА И ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ КЛИЕНТСКОМУ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ
103

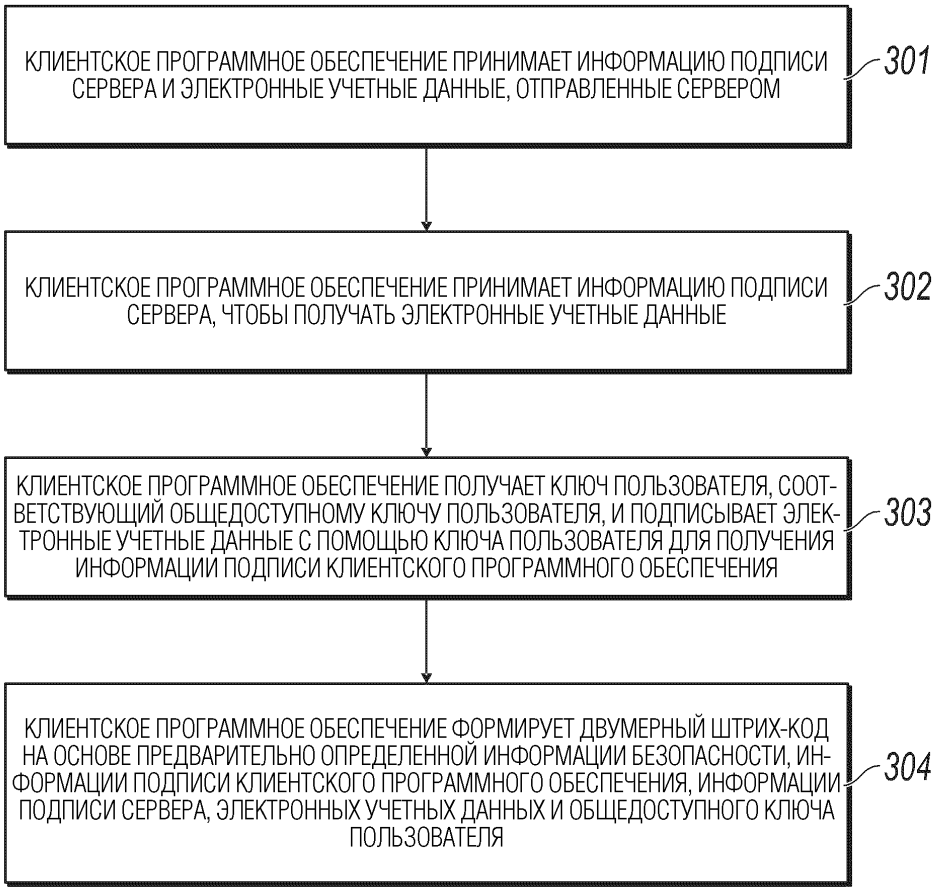
ФИГ. 2

3


201
СЕРВЕР ПРИНИМАЕТ ЗАПРОС НА ПОЛУЧЕНИЕ ЭЛЕКТРОННОГО БИЛЕТА НА КОНЦЕРТ, ОТПРАВЛЕННОГО ALIPAY, ГДЕ ЗАПРОС НА ПОЛУЧЕНИЕ ЭЛЕКТРОННОГО БИЛЕТА НА КОНЦЕРТ ВКЛЮЧАЕТ В СЕБЯ НОМЕР МОБИЛЬНОГО ТЕЛЕФОНА И ВРЕМЯ ДЕЙСТВИЯ УСЛУГИ
202a
СЕРВЕР АНАЛИЗИРУЕТ ЗАПРОС НА ПОЛУЧЕНИЕ ЭЛЕКТРОННОГО БИЛЕТА НА КОНЦЕРТ И ПОЛУЧАЕТ СРОК ДЕЙСТВИЯ УСЛУГИ, ВКЛЮЧЕННЫЙ В ЗАПРОС НА ПОЛУЧЕНИЕ ЭЛЕКТРОННОГО БИЛЕТА НА КОНЦЕРТ
202b
СЕРВЕР АНАЛИЗИРУЕТ ЗАПРОС НА ПОЛУЧЕНИЕ ЭЛЕКТРОННОГО БИЛЕТА НА КОНЦЕРТ И ПОЛУЧАЕТ НОМЕР МОБИЛЬНОГО ТЕЛЕФОНА В ЗАПРОСЕ НА ПОЛУЧЕНИЕ ЭЛЕКТРОННОГО БИЛЕТА НА КОНЦЕРТ
203a
ПРОВЕРЯЕТСЯ, СООТВЕТСТВУЕТ ЛИ СРОК ДЕЙСТВИЯ УСЛУГИ СПЕЦИФИКАЦИИ УСЛУГИ
203b
ПРОВЕРЯЕТСЯ ДОСТОВЕРНОСТЬ НОМЕРА МОБИЛЬНОГО ТЕЛЕФОНА
204
СЕРВЕР ПОЛУЧАЕТ ЭЛЕКТРОННЫЙ БИЛЕТ НА КОНЦЕРТ, КОТОРЫЙ СООТВЕТСТВУЕТ НОМЕРУ МОБИЛЬНОГО ТЕЛЕФОНА И ПОДПИСЫВАЕТ ОБЩЕДОСТУПНЫЙ КЛЮЧ ПОЛЬЗОВАТЕЛЯ ALIPAY И ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ, ИСПОЛЬЗУЯ СЕКРЕТНЫЙ КЛЮЧ СЕРВЕРА, ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ ПОДПИСИ СЕРВЕРА
205
ПЕРЕХВАТЫВАЕТСЯ ЗАПРОС НА ПРИОБРЕТЕНИЕ ЭЛЕКТРОННОГО БИЛЕТА НА КОНЦЕРТ И ОТПРАВЛЯЕТСЯ ЗАПРОС НА ОТКАЗ В ЗАПРОСЕ ALIPAY
206
ОТПРАВЛЯЕТСЯ ИНФОРМАЦИЯ ПОДПИСИ СЕРВЕРА И ЭЛЕКТРОННЫЙ БИЛЕТ НА КОНЦЕРТ В ALIPAY
207
РАСПРОСТРАНЯЕТСЯ ОБЩЕДОСТУПНЫЙ КЛЮЧ, КОТОРЫЙ СООТВЕТСТВУЕТ СЕКРЕТНОМУ КЛЮЧУ СЕРВЕРА, ТАК ЧТО ALIPAY ПРОВЕРЯЕТ ИНФОРМАЦИЮ ПОДПИСИ НА ОСНОВЕ ОБЩЕДОСТУПНОГО КЛЮЧА СЕРВЕРА

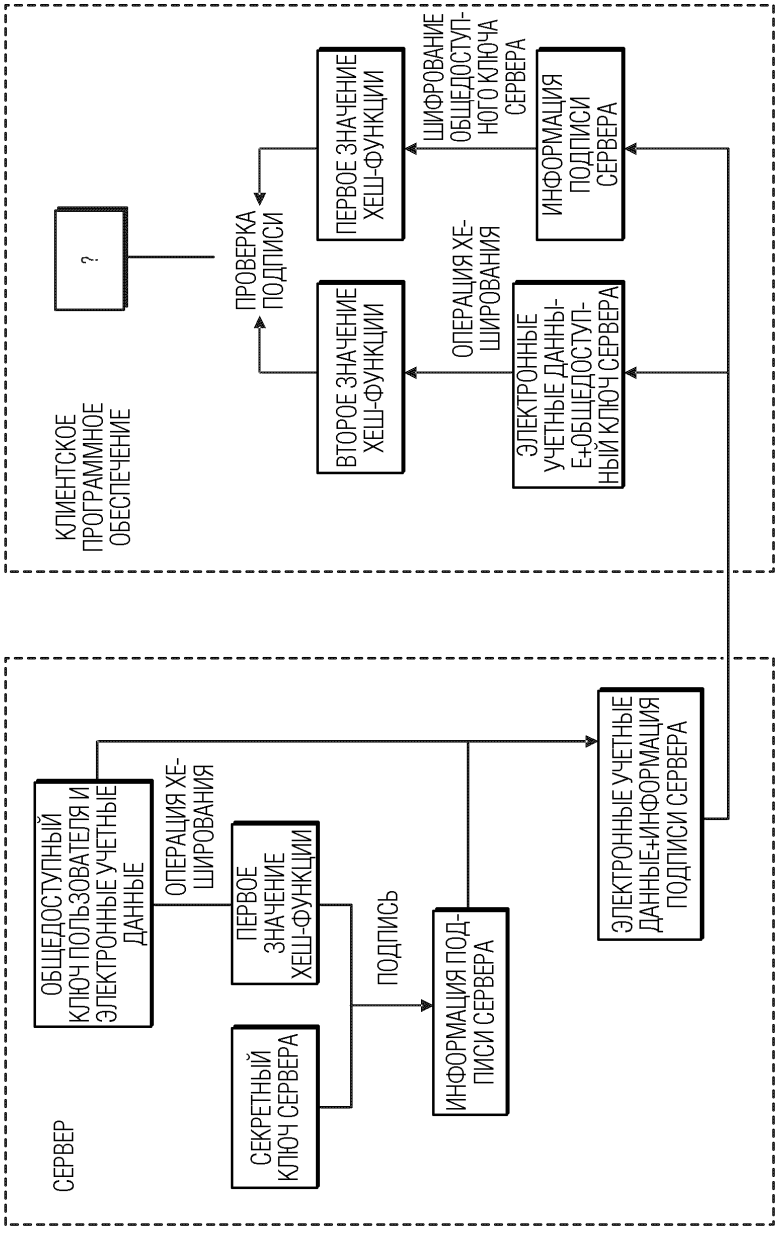
ФИГ. 3

4


КЛИЕНТСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРИНИМАЕТ ИНФОРМАЦИЮ ПОДПИСИ СЕРВЕРА И ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ, ОТПРАВЛЕННЫЕ СЕРВЕРОМ
301
КЛИЕНТСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРИНИМАЕТ ИНФОРМАЦИЮ ПОДПИСИ СЕРВЕРА, ЧТОБЫ ПОЛУЧАТЬ ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ
302
КЛИЕНТСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОЛУЧАЕТ КЛЮЧ ПОЛЬЗОВАТЕЛЯ, СООТВЕТСТВУЮЩИЙ ОБЩЕДОСТУПНОМУ КЛЮЧУ ПОЛЬЗОВАТЕЛЯ, И ПОДПИСЫВАЕТ ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ С ПОМОЩЬЮ КЛЮЧА ПОЛЬЗОВАТЕЛЯ ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ ПОДПИСИ КЛИЕНТСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
303
КЛИЕНТСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ФОРМИРУЕТ ДВУМЕРНЫЙ ШТРИХ-КОД НА ОСНОВЕ ПРЕДВАРИТЕЛЬНО ОПРЕДЕЛЕННОЙ ИНФОРМАЦИИ БЕЗОПАСНОСТИ, ИНФОРМАЦИИ ПОДПИСИ КЛИЕНТСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИНФОРМАЦИИ ПОДПИСИ СЕРВЕРА, ЭЛЕКТРОННЫХ УЧЕТНЫХ ДАННЫХ И ОБЩЕДОСТУПНОГО КЛЮЧА ПОЛЬЗОВАТЕЛЯ
304

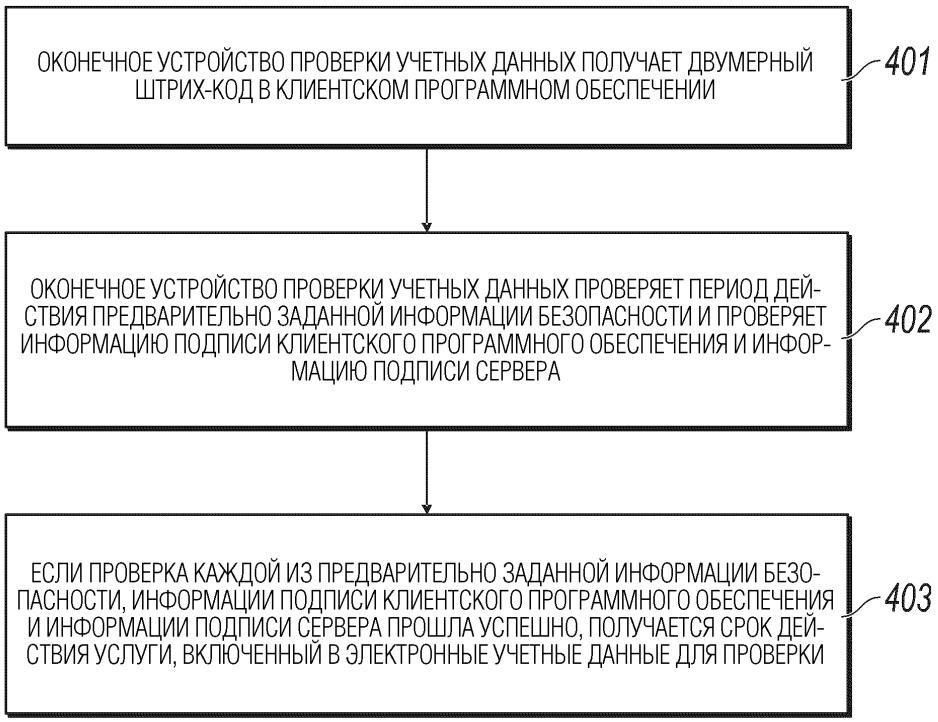
ФИГ. 4

5


КЛИЕНТСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
?
ПРОВЕРКА ПОДПИСИ
ПЕРВОЕ ЗНАЧЕНИЕ ХЕШ-ФУНКЦИИ
ВТОРОЕ ЗНАЧЕНИЕ ХЕШ-ФУНКЦИИ
ШИФРОВАНИЕ ОБЩЕДОСТУПНОГО КЛЮЧА СЕРВЕРА
ОПЕРАЦИЯ ХЕШИРОВАНИЯ
ИНФОРМАЦИЯ ПОДПИСИ СЕРВЕРА
ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ+ОБЩЕДОСТУПНЫЙ КЛЮЧ СЕРВЕРА
СЕРВЕР
ОБЩЕДОСТУПНЫЙ КЛЮЧ ПОЛЬЗОВАТЕЛЯ И ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ
ОПЕРАЦИЯ ХЕШИРОВАНИЯ
ПЕРВОЕ ЗНАЧЕНИЕ ХЕШ-ФУНКЦИИ
СЕКРЕТНЫЙ КЛЮЧ СЕРВЕРА
ПОДПИСЬ
ИНФОРМАЦИЯ ПОДПИСИ СЕРВЕРА
ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ+ИНФОРМАЦИЯ ПОДПИСИ СЕРВЕРА

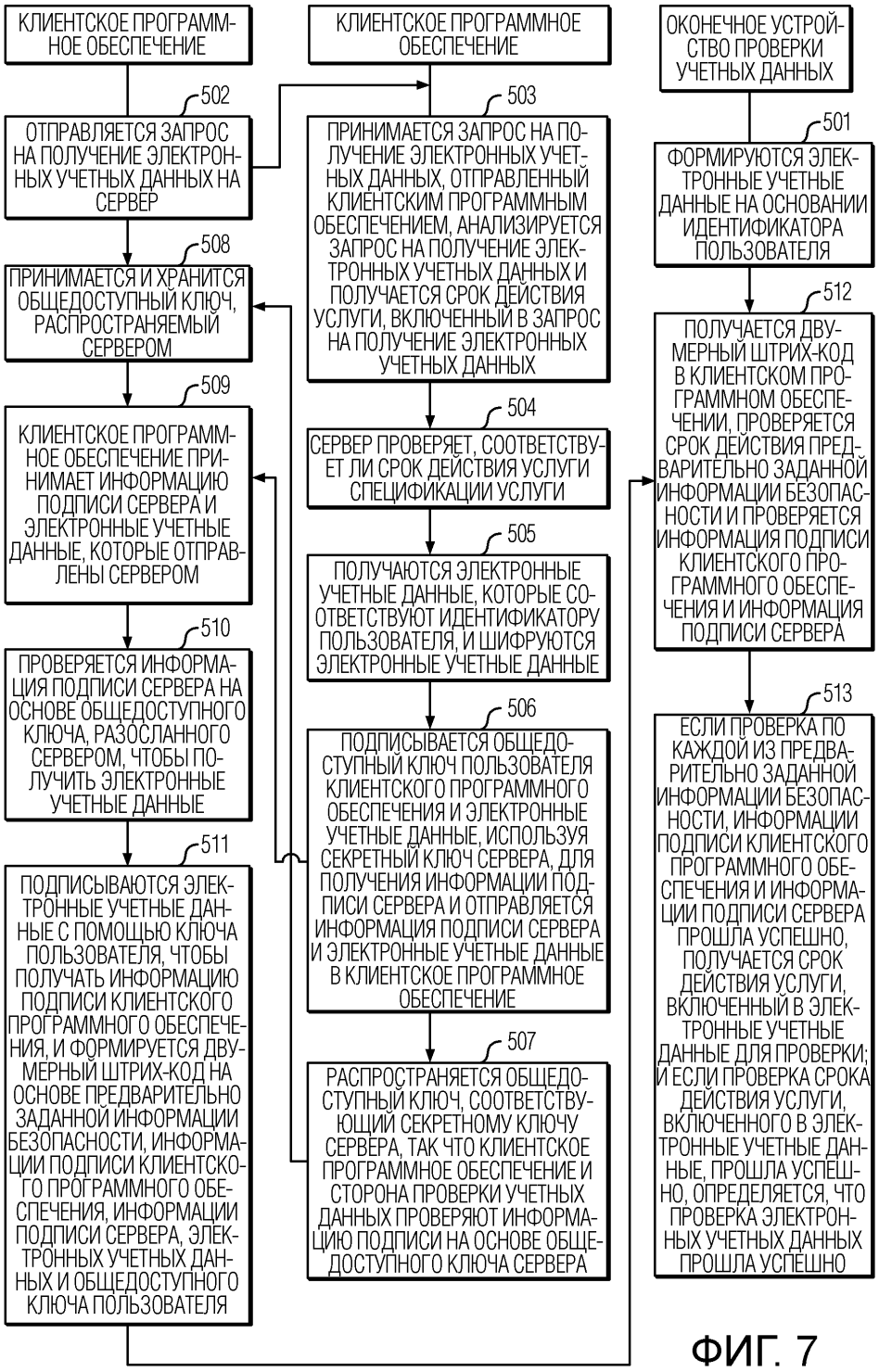
ФИГ. 5

6


ОКОНЕЧНОЕ УСТРОЙСТВО ПРОВЕРКИ УЧЕТНЫХ ДАННЫХ ПОЛУЧАЕТ ДВУМЕРНЫЙ ШТРИХ-КОД В КЛИЕНТСКОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ
401
ОКОНЕЧНОЕ УСТРОЙСТВО ПРОВЕРКИ УЧЕТНЫХ ДАННЫХ ПРОВЕРЯЕТ ПЕРИОД ДЕЙСТВИЯ ПРЕДВАРИТЕЛЬНО ЗАДАННОЙ ИНФОРМАЦИИ БЕЗОПАСНОСТИ И ПРОВЕРЯЕТ ИНФОРМАЦИЮ ПОДПИСИ КЛИЕНТСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИЮ ПОДПИСИ СЕРВЕРА
402
ЕСЛИ ПРОВЕРКА КАЖДОЙ ИЗ ПРЕДВАРИТЕЛЬНО ЗАДАННОЙ ИНФОРМАЦИИ БЕЗОПАСНОСТИ, ИНФОРМАЦИИ ПОДПИСИ КЛИЕНТСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИИ ПОДПИСИ СЕРВЕРА ПРОШЛА УСПЕШНО, ПОЛУЧАЕТСЯ СРОК ДЕЙСТВИЯ УСЛУГИ, ВКЛЮЧЕННЫЙ В ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ ДЛЯ ПРОВЕРКИ
403

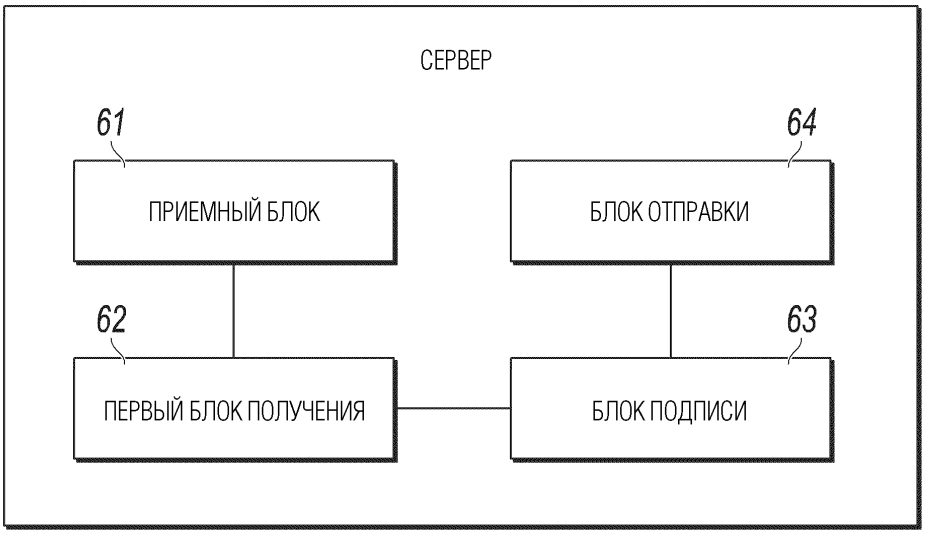
ФИГ. 6

7


КЛИЕНТСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
502
ОТПРАВЛЯЕТСЯ ЗАПРОС НА ПОЛУЧЕНИЕ ЭЛЕКТРОННЫХ УЧЕТНЫХ ДАННЫХ НА СЕРВЕР
508
ПРИНИМАЕТСЯ И ХРАНИТСЯ ОБЩЕДОСТУПНЫЙ КЛЮЧ, РАСПРОСТРАНЯЕМЫЙ СЕРВЕРОМ
509
КЛИЕНТСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРИНИМАЕТ ИНФОРМАЦИЮ ПОДПИСИ СЕРВЕРА И ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ, КОТОРЫЕ ОТПРАВЛЕНЫ СЕРВЕРОМ
510
ПРОВЕРЯЕТСЯ ИНФОРМАЦИЯ ПОДПИСИ СЕРВЕРА НА ОСНОВЕ ОБЩЕДОСТУПНОГО КЛЮЧА, РАЗОСЛАННОГО СЕРВЕРОМ, ЧТОБЫ ПОЛУЧИТЬ ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ
511
ПОДПИСЫВАЮТСЯ ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ С ПОМОЩЬЮ КЛЮЧА ПОЛЬЗОВАТЕЛЯ, ЧТОБЫ ПОЛУЧАТЬ ИНФОРМАЦИЮ ПОДПИСИ КЛИЕНТСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, И ФОРМИРУЕТСЯ ДВУМЕРНЫЙ ШТРИХ-КОД НА ОСНОВЕ ПРЕДВАРИТЕЛЬНО ЗАДАННОЙ ИНФОРМАЦИИ БЕЗОПАСНОСТИ, ИНФОРМАЦИИ ПОДПИСИ КЛИЕНТСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИНФОРМАЦИИ ПОДПИСИ СЕРВЕРА, ЭЛЕКТРОННЫХ УЧЕТНЫХ ДАННЫХ И ОБЩЕДОСТУПНОГО КЛЮЧА ПОЛЬЗОВАТЕЛЯ
КЛИЕНТСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
503
ПРИНИМАЕТСЯ ЗАПРОС НА ПОЛУЧЕНИЕ ЭЛЕКТРОННЫХ УЧЕТНЫХ ДАННЫХ, ОТПРАВЛЕННЫЙ КЛИЕНТСКИМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ, АНАЛИЗИРУЕТСЯ ЗАПРОС НА ПОЛУЧЕНИЕ ЭЛЕКТРОННЫХ УЧЕТНЫХ ДАННЫХ И ПОЛУЧАЕТСЯ СРОК ДЕЙСТВИЯ УСЛУГИ, ВКЛЮЧЕННЫЙ В ЗАПРОС НА ПОЛУЧЕНИЕ ЭЛЕКТРОННЫХ УЧЕТНЫХ ДАННЫХ
504
СЕРВЕР ПРОВЕРЯЕТ, СООТВЕТСТВУЕТ ЛИ СРОК ДЕЙСТВИЯ УСЛУГИ СПЕЦИФИКАЦИИ УСЛУГИ
505
ПОЛУЧАЮТСЯ ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ, КОТОРЫЕ СООТВЕТСТВУЮТ ИДЕНТИФИКАТОРУ ПОЛЬЗОВАТЕЛЯ, И ШИФРУЮТСЯ ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ
506
ПОДПИСЫВАЕТСЯ ОБЩЕДОСТУПНЫЙ КЛЮЧ ПОЛЬЗОВАТЕЛЯ КЛИЕНТСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ, ИСПОЛЬЗУЯ СЕКРЕТНЫЙ КЛЮЧ СЕРВЕРА, ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ ПОДПИСИ СЕРВЕРА И ОТПРАВЛЯЕТСЯ ИНФОРМАЦИЯ ПОДПИСИ СЕРВЕРА И ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ В КЛИЕНТСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
507
РАСПРОСТРАНЯЕТСЯ ОБЩЕДОСТУПНЫЙ КЛЮЧ, СООТВЕТСТВУЮЩИЙ СЕКРЕТНОМУ КЛЮЧУ СЕРВЕРА, ТАК ЧТО КЛИЕНТСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И СТОРОНА ПРОВЕРКИ УЧЕТНЫХ ДАННЫХ ПРОВЕРЯЮТ ИНФОРМАЦИЮ ПОДПИСИ НА ОСНОВЕ ОБЩЕДОСТУПНОГО КЛЮЧА СЕРВЕРА
ОКОНЕЧНОЕ УСТРОЙСТВО ПРОВЕРКИ УЧЕТНЫХ ДАННЫХ
501
ФОРМИРУЮТСЯ ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ НА ОСНОВАНИИ ИДЕНТИФИКАТОРА ПОЛЬЗОВАТЕЛЯ
512
ПОЛУЧАЕТСЯ ДВУМЕРНЫЙ ШТРИХ-КОД В КЛИЕНТСКОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ, ПРОВЕРЯЕТСЯ СРОК ДЕЙСТВИЯ ПРЕДВАРИТЕЛЬНО ЗАДАННОЙ ИНФОРМАЦИИ БЕЗОПАСНОСТИ И ПРОВЕРЯЕТСЯ ИНФОРМАЦИЯ ПОДПИСИ КЛИЕНТСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИЯ ПОДПИСИ СЕРВЕРА
513
ЕСЛИ ПРОВЕРКА ПО КАЖДОЙ ИЗ ПРЕДВАРИТЕЛЬНО ЗАДАННОЙ ИНФОРМАЦИИ БЕЗОПАСНОСТИ, ИНФОРМАЦИИ ПОДПИСИ КЛИЕНТСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИИ ПОДПИСИ СЕРВЕРА ПРОШЛА УСПЕШНО, ПОЛУЧАЕТСЯ СРОК ДЕЙСТВИЯ УСЛУГИ, ВКЛЮЧЕННЫЙ В ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ ДЛЯ ПРОВЕРКИ; И ЕСЛИ ПРОВЕРКА СРОКА ДЕЙСТВИЯ УСЛУГИ, ВКЛЮЧЕННОГО В ЭЛЕКТРОННЫЕ УЧЕТНЫЕ ДАННЫЕ, ПРОШЛА УСПЕШНО, ОПРЕДЕЛЯЕТСЯ, ЧТО ПРОВЕРКА ЭЛЕКТРОННЫХ УЧЕТНЫХ ДАННЫХ ПРОШЛА УСПЕШНО

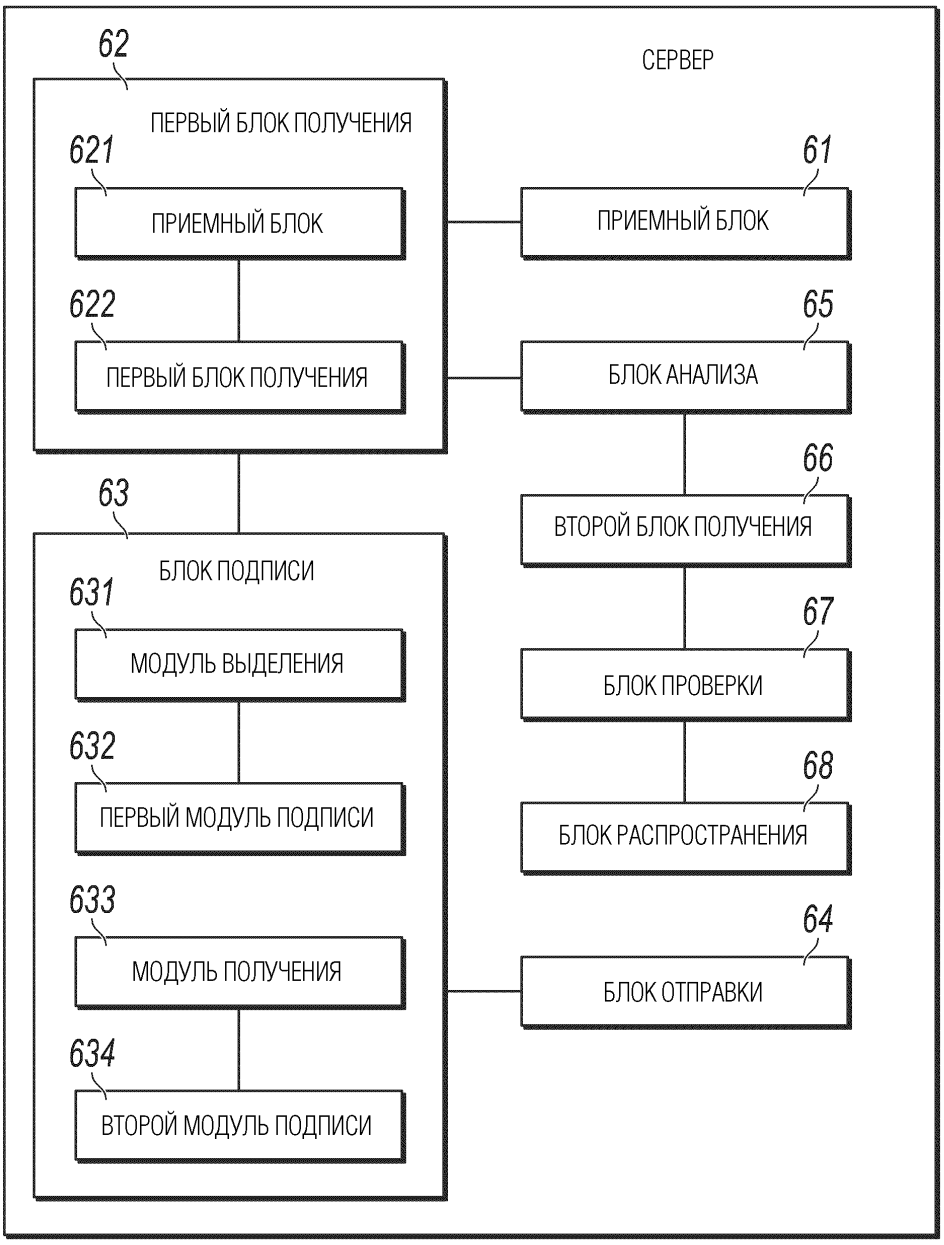
ФИГ. 7

8


СЕРВЕР
61
ПРИЕМНЫЙ БЛОК
64
БЛОК ОТПРАВКИ
62
ПЕРВЫЙ БЛОК ПОЛУЧЕНИЯ
63
БЛОК ПОДПИСИ

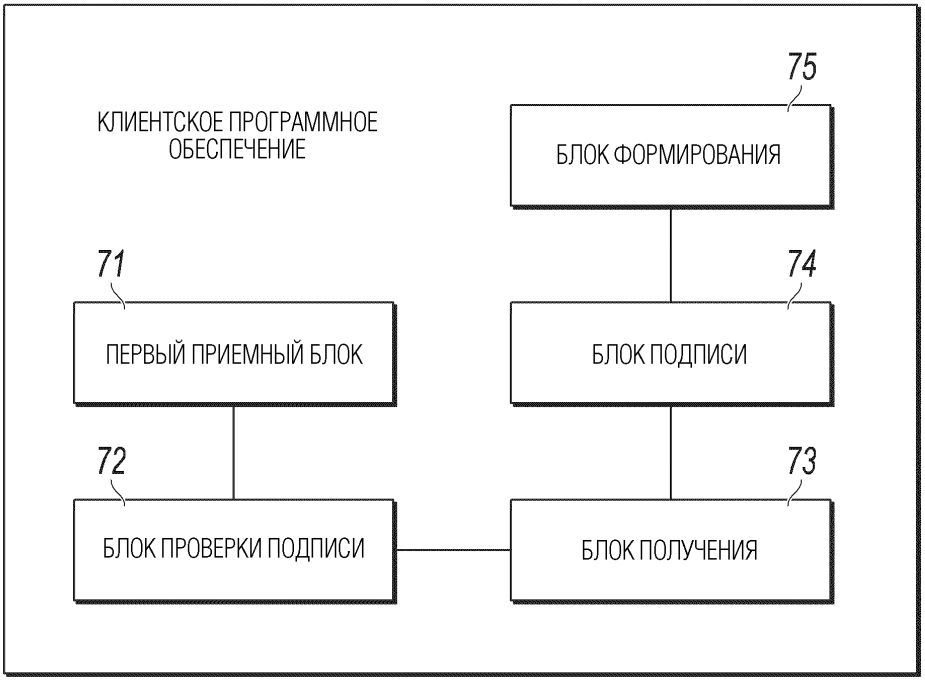
ФИГ. 8

9


62
ПЕРВЫЙ БЛОК ПОЛУЧЕНИЯ
621
ПРИЕМНЫЙ БЛОК
622
ПЕРВЫЙ БЛОК ПОЛУЧЕНИЯ
63
БЛОК ПОДПИСИ
631
МОДУЛЬ ВЫДЕЛЕНИЯ
632
ПЕРВЫЙ МОДУЛЬ ПОДПИСИ
633
МОДУЛЬ ПОЛУЧЕНИЯ
634
ВТОРОЙ МОДУЛЬ ПОДПИСИ
СЕРВЕР
61
ПРИЕМНЫЙ БЛОК
65
БЛОК АНАЛИЗА
66
ВТОРОЙ БЛОК ПОЛУЧЕНИЯ
67
БЛОК ПРОВЕРКИ
68
БЛОК РАСПРОСТРАНЕНИЯ
64
БЛОК ОТПРАВКИ

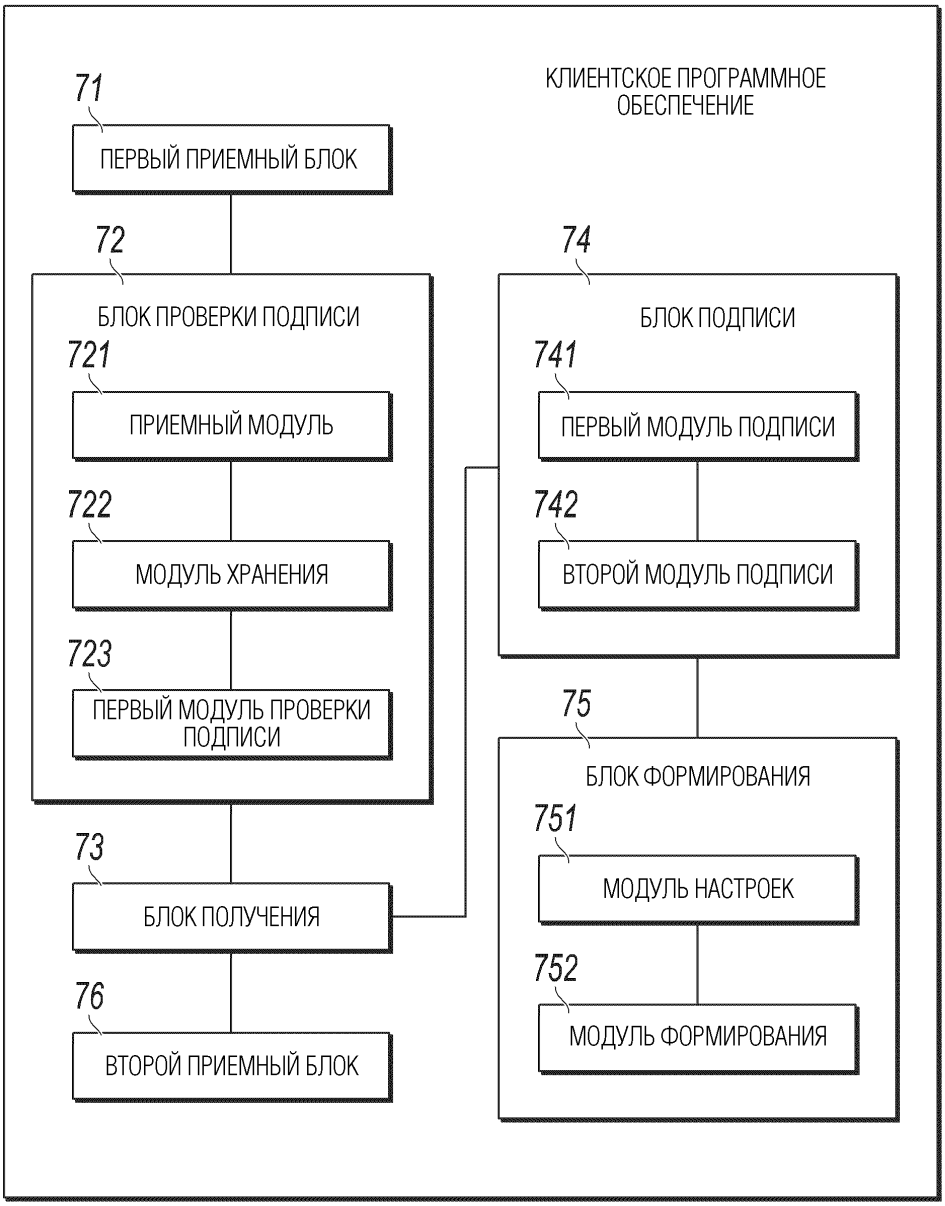
ФИГ. 9

10


КЛИЕНТСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
75
БЛОК ФОРМИРОВАНИЯ
71
ПЕРВЫЙ ПРИЕМНЫЙ БЛОК
74
БЛОК ПОДПИСИ
72
БЛОК ПРОВЕРКИ ПОДПИСИ
73
БЛОК ПОЛУЧЕНИЯ

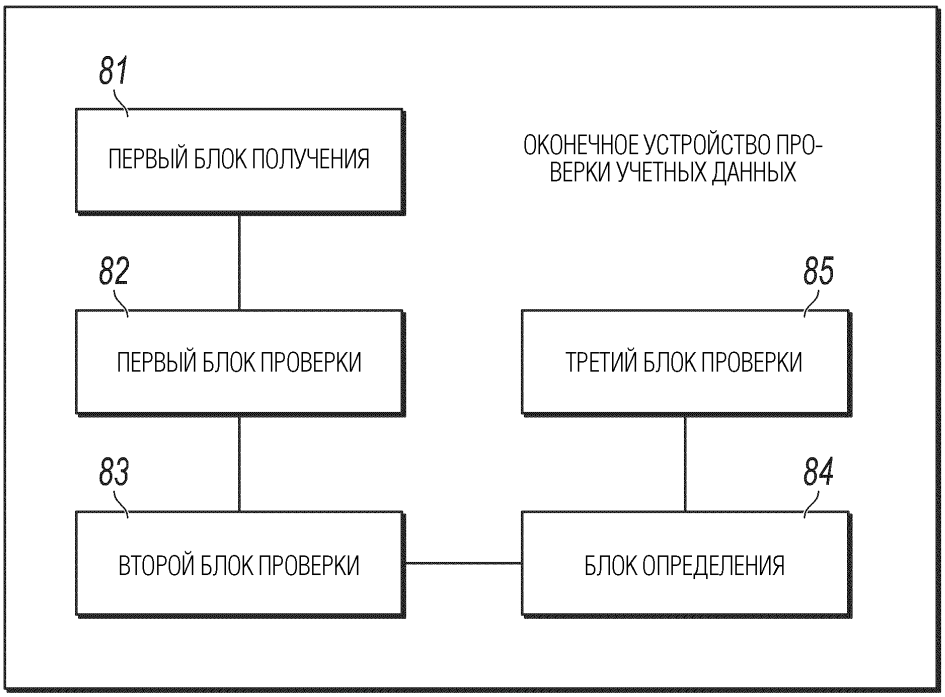
ФИГ. 10

11


КЛИЕНТСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
71
ПЕРВЫЙ ПРИЕМНЫЙ БЛОК
72
БЛОК ПРОВЕРКИ ПОДПИСИ
721
ПРИЕМНЫЙ МОДУЛЬ
722
МОДУЛЬ ХРАНЕНИЯ
723
ПЕРВЫЙ МОДУЛЬ ПРОВЕРКИ ПОДПИСИ
73
БЛОК ПОЛУЧЕНИЯ
76
ВТОРОЙ ПРИЕМНЫЙ БЛОК
74
БЛОК ПОДПИСИ
741
ПЕРВЫЙ МОДУЛЬ ПОДПИСИ
742
ВТОРОЙ МОДУЛЬ ПОДПИСИ
75
БЛОК ФОРМИРОВАНИЯ
751
МОДУЛЬ НАСТРОЕК
752
МОДУЛЬ ФОРМИРОВАНИЯ

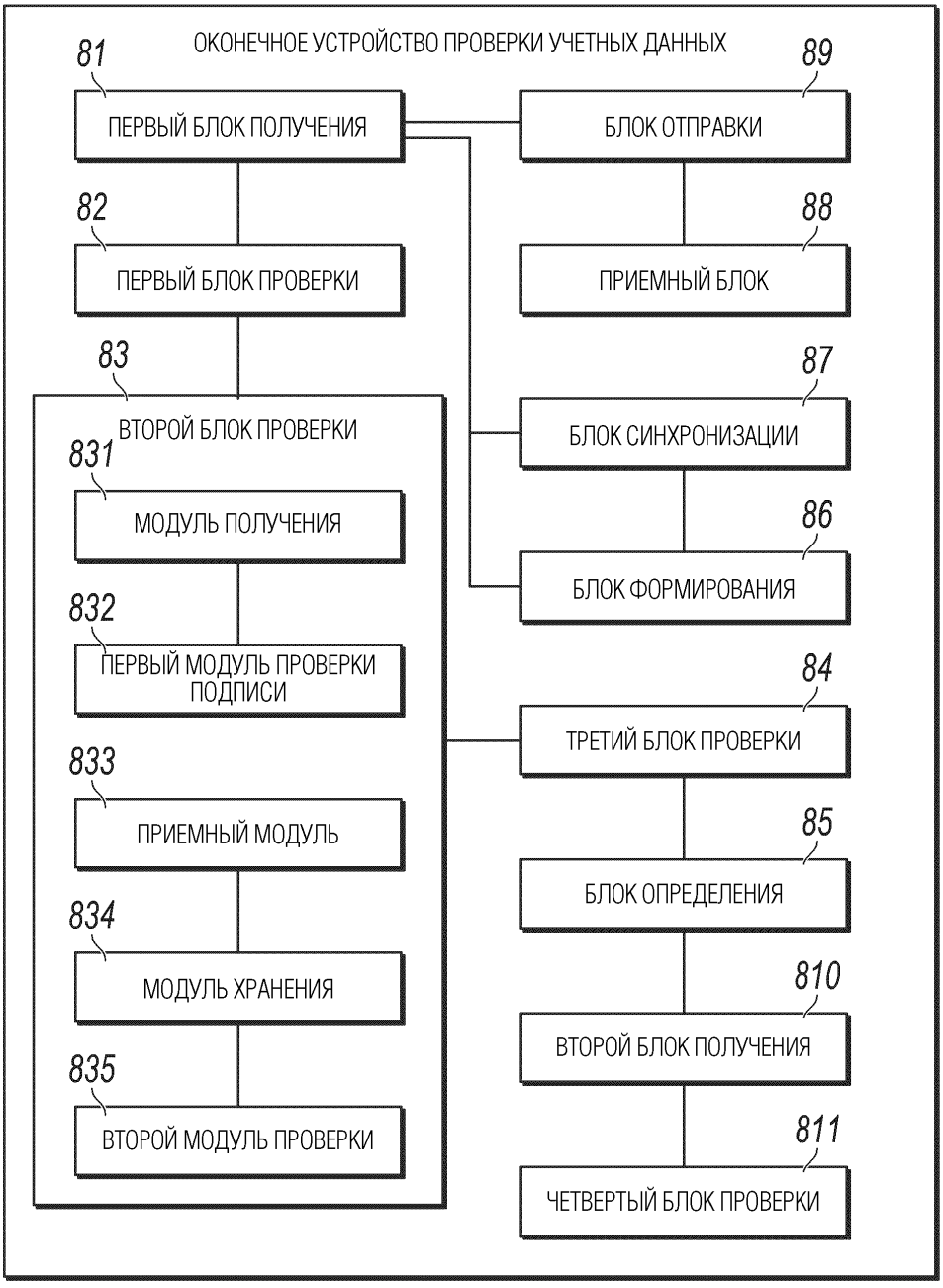
ФИГ. 11

12


81
ПЕРВЫЙ БЛОК ПОЛУЧЕНИЯ
ОКОНЕЧНОЕ УСТРОЙСТВО ПРОВЕРКИ УЧЕТНЫХ ДАННЫХ
82
ПЕРВЫЙ БЛОК ПРОВЕРКИ
85
ТРЕТИЙ БЛОК ПРОВЕРКИ
83
ВТОРОЙ БЛОК ПРОВЕРКИ
84
БЛОК ОПРЕДЕЛЕНИЯ

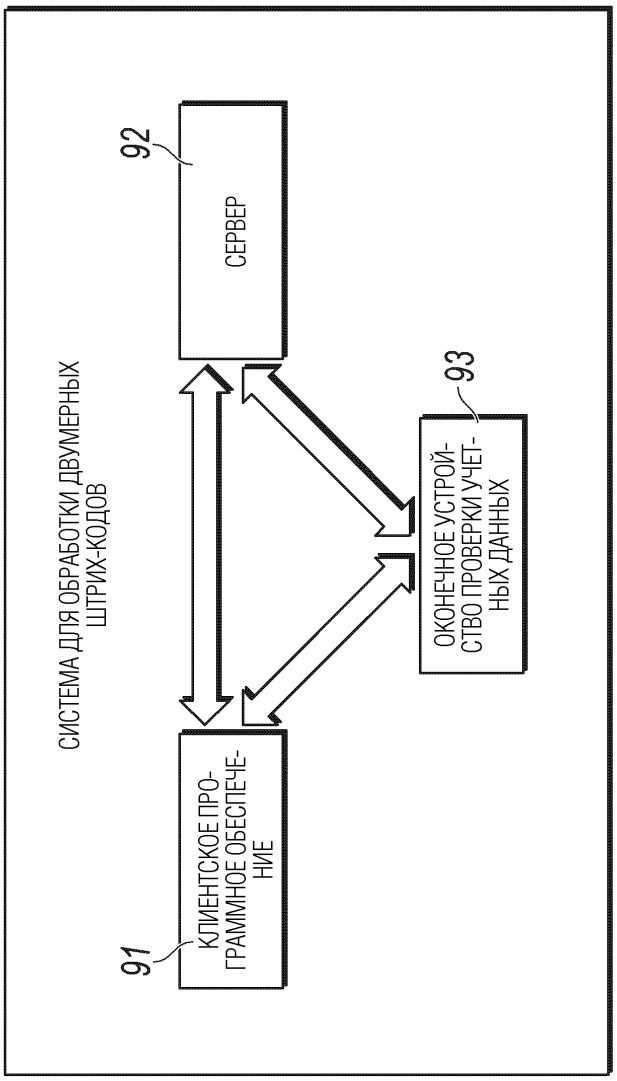
ФИГ. 12

13


ОКОНЕЧНОЕ УСТРОЙСТВО ПРОВЕРКИ УЧЕТНЫХ ДАННЫХ
81
ПЕРВЫЙ БЛОК ПОЛУЧЕНИЯ
82
ПЕРВЫЙ БЛОК ПРОВЕРКИ
83
ВТОРОЙ БЛОК ПРОВЕРКИ
831
МОДУЛЬ ПОЛУЧЕНИЯ
832
ПЕРВЫЙ МОДУЛЬ ПРОВЕРКИ ПОДПИСИ
833
ПРИЕМНЫЙ МОДУЛЬ
834
МОДУЛЬ ХРАНЕНИЯ
835
ВТОРОЙ МОДУЛЬ ПРОВЕРКИ
89
БЛОК ОТПРАВКИ
88
ПРИЕМНЫЙ БЛОК
87
БЛОК СИНХРОНИЗАЦИИ
86
БЛОК ФОРМИРОВАНИЯ
84
ТРЕТИЙ БЛОК ПРОВЕРКИ
85
БЛОК ОПРЕДЕЛЕНИЯ
810
ВТОРОЙ БЛОК ПОЛУЧЕНИЯ
811
ЧЕТВЕРТЫЙ БЛОК ПРОВЕРКИ

ФИГ. 13

14


СИСТЕМА ДЛЯ ОБРАБОТКИ ДВУМЕРНЫХ ШТРИХ-КОДОВ
92
СЕРВЕР
93
ОКОНЕЧНОЕ УСТРОЙСТВО ПРОВЕРКИ УЧЕТНЫХ ДАННЫХ
91
КЛИЕНТСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

ФИГ. 14