РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 556 453**(13) **C2**

(51) МПК
G06Q 20/00 (2012.01)
H04W 12/06 (2009.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2011153714/08, 02.06.2010**

(24) Дата начала отсчета срока действия патента:
02.06.2010

Приоритет(ы):
(30) Конвенционный приоритет:
03.06.2009 US 61/183,631

(43) Дата публикации заявки: **20.07.2013** Бюл. № **20**

(45) Опубликовано: **10.07.2015** Бюл. № **19**

(56) Список документов, цитированных в отчете о поиске: **US 2004/0248554 A1, 09.12.2004 . US 2007/0198410 A1, 23.08.2007 . US 2002/0007343 A1, 17.01.2002 . US 2004/0230536 A1, 18.11.2004 . RU 2352991 C2, 20.04.2009**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **10.01.2012**

(86) Заявка PCT:
US 2010/037054 (02.06.2010)

(87) Публикация заявки PCT:
WO 2010/141573 (09.12.2010)

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

(72) Автор(ы):
КУЛПАТИ Ашиш (IN),
РАДЖУРКАР Панкадж (IN),
САМ ООН Соон Гуан (SG),
ФИШЕР Дуглас (US),
ДИММИК Джеймс Дин (US),
ДОМИНГЕС Бенедикто Эрнандез (US),
КИМ Ин-Тчанг (SG)

(73) Патентообладатель(и):
ВИЗА ИНТЕРНЭШНЛ СЕРВИС АССОСИЭЙШН (US)

(54) СИСТЕМА И СПОСОБ ОБЕСПЕЧЕНИЯ АУТЕНТИФИКАЦИИ ДЛЯ ТРАНЗАКЦИЙ БЕЗ НАЛИЧИЯ КАРТЫ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО УСТРОЙСТВА

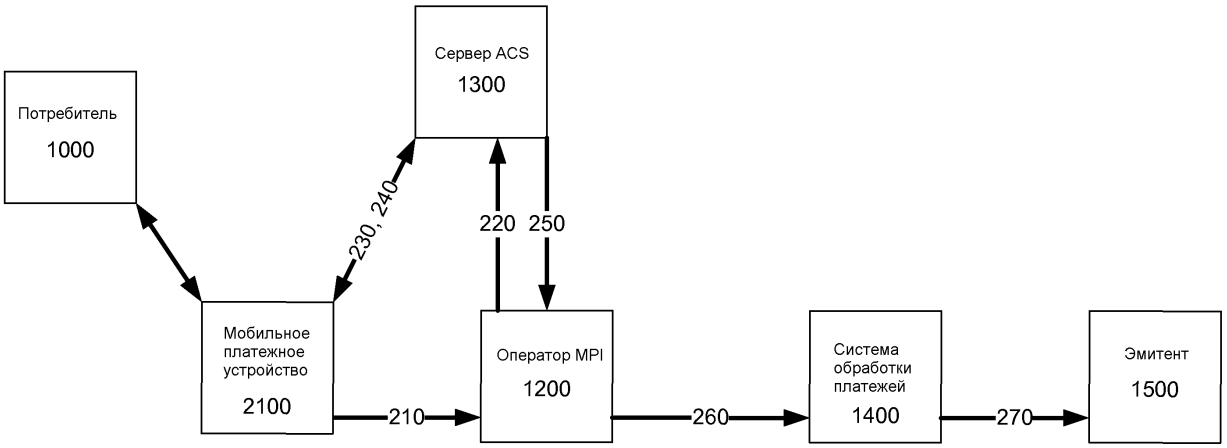
(57) Реферат:

Изобретение относится к устройству, способам и компьютеру для аутентификации потребителя и проведения платежной транзакции. Технический результат заключается в повышении скорости проведения платежной транзакции. Устройство содержит процессор, носитель данных, присоединенный к процессору и содержащий набор инструкций, при выполнении которых процессором устройство аутентифицирует потребителя посредством регистрации мобильного устройства и связи мобильного устройства с платежным счетом потребителя, аутентификации регистрации мобильного устройства с использованием идентификационных данных, ранее предоставленных потребителем и связанных с платежным счетом, приема данных, инициирующих платежную транзакцию, определения, что платежная транзакция была инициирована с использованием мобильного устройства и определения, основываясь на аутентификации регистрации мобильного устройства, что платежная транзакция аутентифицирована для платежного счета с

RU 2556453 C2

RU 2556453 C2

использованием мобильного устройства. 5 н. и 36 з.п. ф-лы, 6 ил.



Фиг. 2

RU 2556453 C2

RU 2556453 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 556 453** (13) **C2**

(51) Int. Cl.
G06Q 20/00 (2012.01)
H04W 12/06 (2009.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2011153714/08, 02.06.2010**

(24) Effective date for property rights:
02.06.2010

Priority:
(30) Convention priority:
03.06.2009 US 61/183,631

(43) Application published: **20.07.2013** Bull. № **20**

(45) Date of publication: **10.07.2015** Bull. № **19**

(85) Commencement of national phase: **10.01.2012**

(86) PCT application:
US 2010/037054 (02.06.2010)

(87) PCT publication:
WO 2010/141573 (09.12.2010)

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

(72) Inventor(s):
KULPATI Ashish (IN),
RADZhURKAR Pankadzh (IN),
SAM OON Soon Guan (SG),
FIShER Duglas (US),
DIMMIK Dzhejms Din (US),
DOMINGES Benedikto Ehrnandez (US),
KIM In-Tchang (SG)

(73) Proprietor(s):
VIZA INTERNEhShNL SERVIS ASSOSIEhJShN (US)

(54) SYSTEM AND METHOD FOR AUTHENTICATION OF TRANSACTIONS WITHOUT CAR WITH HELP OF MOBILE DEVICE

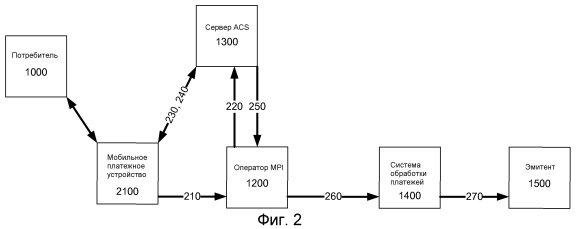
(57) Abstract:

FIELD: physics, computation hardware.

SUBSTANCE: invention relates to authentication of the user and performance of payment transaction. Proposed device comprises processor, data carrier connected thereto and including the set of instructions. Execution of said instructions by said processor makes this device authenticate the user by registration of mobile device and communication of mobile device with the user payment account. Mobile device is registered is authenticated with the use of identification data issued by the user and related with payment account. Data initiating the payment transaction is received to define is payment transaction is initiated with the help of mobile device. Proceeding from the mobile device registration authentication payment transaction is authenticated for payment account with the use of mobile device.

EFFECT: higher rate of payment transaction.

41 cl, 6 dwg



Фиг. 2

RU 2556453 C2

RU 2556453 C2

ПЕРЕКРЕСТНЫЕ ССЫЛКИ НА РОДСТВЕННЫЕ ЗАЯВКИ

Эта заявка притязает на приоритет предварительной заявки на патент США № 61/183631, поданной 3 июня 2009 года, полное раскрытие которой включено в настоящий документ посредством ссылки во всей своей полноте.

УРОВЕНЬ ТЕХНИКИ

Потребительские платежные устройства, такие как дебетовые карты или кредитные карты, используются миллионами людей во всем мире для обеспечения коммерческих транзакций различных типов. В типичной транзакции, включающей в себя покупку продукта или услуги в торговом местоположении, платежное устройство представляется в терминале точки продажи ("терминал POS"), расположенном в месте ведения бизнеса продавца. Терминал точки продажи может представлять собой устройство считывания карт или подобное устройство, которое может осуществлять доступ к данным, хранящимся на платежном устройстве, причем эти данные могут включать в себя, например, идентификационные данные потребителя, данные аутентификации или данные счета. Некоторые или все данные, считанные с платежного устройства, предоставляются системе транзакций или обработки данных продавца и затем обслуживающей стороне, которая обычно является банком или другим учреждением, которое управляет счетом продавца. Данные, предоставленные обслуживающей стороне, затем могут быть предоставлены системе или сети обработки платежей (например, обработчику платежей), которая обрабатывает данные, чтобы помочь в определении, должна ли транзакция быть авторизована сетью, и помогает в выполнении функций произведения расчетов и урегулирования счета для транзакции. Части транзакции по принятию решения об авторизации, произведению расчетов и урегулированию транзакции также могут включать в себя взаимодействие и/или передачу данных между системой или сетью обработки платежей и банком или учреждением, которое выпустило платежное устройство потребителю (эмитент). Транзакции, в которых потребительское платежное устройство представляется продавцу или к нему осуществляет доступ терминалом точки продажи, называют "транзакциями с наличием карты", поскольку платежное устройство находится в том же самом физическом местоположении, где находится продавец или терминал.

В дополнение к транзакциям с наличием карты потребитель также может инициировать транзакцию в ситуации, в которой платежное устройство не находится в том же самом физическом местоположении, где находится продавец или терминал, и вместо этого соответствующие данные предоставляются по системе связи продавцу ("транзакция без наличия карты"). Например, транзакция без наличия карты, включающая в себя покупку продукта или услуги, может быть инициирована потребителем посредством предоставления платежных данных из удаленного местоположения продавцу по сети, такой как Интернет. Транзакции этого типа обычно инициируются с использованием вычислительного устройства, такого как персональный компьютер или переносной компьютер. Транзакции без наличия карты также могут быть инициированы или выполнены с использованием мобильного платежного устройства, такого как мобильный телефон, в случае с которым связь с продавцом или системой обработки данных может произойти по сети сотовой или беспроводной связи. Таким образом, среди прочих способов, платежная информация для транзакции может быть предоставлена с использованием платежного устройства и терминала точки продажи или может быть предоставлена продавцу с использованием удаленно расположенного платежного устройства.

Учитывая большое количество транзакций и вовлеченных сумм денег, обнаружение

и предотвращение мошенничества является важным аспектом любой системы обработки транзакций. Чтобы обратиться к этой проблеме, платежные процессоры и т.д., вовлеченные в авторизацию транзакции, обычно требуют, чтобы пользователь обеспечил одну или более форм аутентификации или идентификации перед авторизацией транзакции. В транзакции с наличием карты продавец может просто попросить у потребителя другую форму идентификации, например документ с фотографией (водительские права, паспорт и т.д.), для обеспечения дополнительной гарантии, что человек авторизован для использования представленного платежного устройства.

Однако в случае транзакции без наличия карты (такой как транзакция электронной коммерции, проводимая по Интернету, или транзакции, которая выполняется с использованием мобильного платежного устройства) продавец не может быть настолько уверен, что человек, который пытается использовать платежное устройство, является человеком, который авторизован для использования этого устройства. Удаленная природа транзакции делает документ с фотографией или другой вид идентификации непрактичным и ненадежным в качестве средства аутентификации потребителя. Кроме того, запрос дополнительной части, предположительно, конфиденциальных данных от человека, пытающегося использовать платежное устройство, может быть недостаточным для проверки, что человек авторизован для использования платежного устройства. Это происходит потому, что в некоторых ситуациях дополнительные данные могли быть получены тем же самым мошенническим путем, как и данные счета платежного устройства (например, посредством ненадлежащего получения доступа к компьютеру человека, который хранит данные счета и другие конфиденциальные данные). Кроме того, как в платежных, так и в не платежных транзакциях (таких, которые могут иметь место в торговле, согласовании договоров и т.д.) каждая сторона в транзакции обычно предпочитает иметь средство аутентификации идентификационной информации и данных, имеющих отношение к другим сторонам в соглашении или транзакции. Желательно предотвратить мошенничество, искажения или более позднее аннулирование соглашения. Таким образом, желательно иметь надежные способы аутентификации стороны в транзакции в случаях, когда платежное устройство или сторона не присутствуют в местоположении продавца или другой стороны в транзакции или соглашении. Если возможно, также желательно использовать элементы существующих систем аутентификации платежных устройств, которые используются для транзакций с наличием карты, для выполнения некоторых или всех операций аутентификации для транзакций без наличия карты, поскольку это уменьшит стоимость и сложность дополнительных процессов аутентификации.

С учетом изложенного желательно иметь систему и соответствующие устройства и способы аутентификации потребителя, который участвует в удаленной транзакции, такой как транзакция без наличия карты, проводимая по сети сотовой или беспроводной связи с использованием мобильного платежного устройства. Кроме того, желательно, чтобы система аутентификации была относительно легка для реализации и использования, и дать потребителям возможность зарегистрировать мобильное платежное устройство для использования в транзакции и аутентифицироваться во время транзакции. Кроме того, было бы желательно, чтобы система, устройства и способы не требовали существенных инвестиций новых ресурсов для реализации и обеспечивали высокий уровень функциональной совместимости между участниками системы. Дополнительно было бы желательно, чтобы существующие системы аутентификации для сетевых транзакций электронной коммерции могли быть усилены для предоставления возможности мобильным платежным устройствам проводить транзакции без наличия

карты по мобильному каналу с использованием некоторых или всех тех же самых системных элементов. Варианты воплощения изобретения направлены на решение этих и других проблем по отдельности и совместно.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

Варианты воплощения настоящего изобретения направлены на системы и соответствующие устройства и способы аутентификации участников, вовлеченных в транзакцию без наличия карты. В таких транзакциях один участник транзакции (и, следовательно, платежное устройство этого участника) находится в удаленном местоположении относительно другого участника транзакции. Это может создать неуверенность относительно идентификационной информации удаленно расположенного участника или относительно подлинности данных, предоставленных участником. Система, устройства и способы изобретения могут использоваться в качестве части выполнения платежных и не платежных транзакций и подходят для использования в транзакциях электронной коммерции, проводимых с использованием мобильного платежного устройства, такого как мобильный телефон.

Один аспект настоящего изобретения состоит в том, что оно может быть реализовано с использованием элементов инфраструктуры, которые используются в настоящее время для аутентификации платежных устройств и участников транзакций с наличием карты, и поэтому не требует полностью нового набора систем, процессов или операций. Таким образом, варианты воплощения настоящего изобретения могут позволить банкам и другим поставщикам услуг мобильных платежей усилить существующие платформы аутентификации для обеспечения службы аутентификации для транзакций без наличия карты, инициируемых с использованием мобильных платежных устройств. Это уменьшает стоимость обеспечения услуг мобильных платежей потребителям и может увеличить признание таких услуг, поскольку потребители и другие объекты, включенные в процесс платежной транзакции, уже будут знакомы со многими, если не всеми, системами и используемыми процессами. Кроме того, варианты воплощения настоящего изобретения могут использоваться потребителями и другими объектами, вовлеченными в платежную транзакцию, для обеспечения улучшенной безопасности (включающей в себя несколько уровней безопасности при аутентификации потребителя, проводящего транзакцию), увеличения скорости обработки транзакций и большего удобства для потребителей, чем это было возможно в отсутствие изобретения.

В некоторых вариантах воплощения система, устройство и способ изобретения включают в себя инфраструктуру и процессы для обеспечения потребителю возможности зарегистрировать свой номер мобильного телефона и связывать этот номер с платежным счетом. После регистрации потребитель может использовать свой мобильный телефон, чтобы инициировать или выполнить один или более этапов платежной транзакции. Платежная транзакция распознается как инициированная или выполненная посредством мобильного телефона, и в ответ сервер может аутентифицировать транзакцию на основе номера мобильного телефона и предшествующей регистрации и процесса аутентификации. В других вариантах воплощения сервер может распознать платежную транзакцию как инициированную или выполненную посредством мобильного телефона и в ответ осуществить контакт с потребителем, использующим мобильный телефон, чтобы запросить подтверждение желания потребителя выполнить транзакцию.

В одном варианте воплощения настоящее изобретение направлено на устройство для аутентификации потребителя, проводящего платежную транзакцию с использованием мобильного устройства, причем устройство включает в себя процессор, запрограммированный для исполнения набора инструкций, носитель данных,

присоединенный к процессору, и причем набор инструкций содержится на носителе данных, при этом, когда набор инструкций исполняется процессором, устройство аутентифицирует потребителя посредством регистрации мобильного устройства и связи мобильного устройства с платежным счетом потребителя, аутентификации регистрации мобильного устройства с использованием идентификационных данных, предварительно предоставленных потребителем и связанных с платежным счетом, приема данных, инициирующих платежную транзакцию, и определения, что платежная транзакция была инициирована с использованием мобильного устройства.

В другом варианте воплощения настоящее изобретение направлено на способ аутентификации потребителя, проводящего платежную транзакцию с использованием мобильного устройства, причем способ содержит этапы, на которых принимают данные, идентифицирующие мобильное устройство, и данные, идентифицирующие платежный счет потребителя, аутентифицируют мобильное устройство с использованием идентификационных данных, предварительно предоставленных потребителем и связанных с платежным счетом, принимают данные, инициирующие платежную транзакцию, и определяют, что платежная транзакция была инициирована с использованием мобильного устройства.

В еще одном варианте воплощения настоящее изобретение направлено на способ проведения платежной транзакции, причем способ содержит этапы, на которых связывают платежный счет потребителя и первые идентификационные данные потребителя, при этом первые идентификационные данные потребителя используются потребителем для одобрения платежных транзакций, сделанных с использованием платежного счета потребителя, принимают данные, идентифицирующие мобильное устройство, и данные, идентифицирующие платежный счет потребителя, выполняют запрос к потребителю предоставить первые идентификационные данные потребителя, аутентифицируют мобильное устройство, если ответ на запрос представляет собой первые идентификационные данные потребителя, принимают данные, инициирующие платежную транзакцию, определяют, что платежная транзакция была инициирована с использованием мобильного устройства, и в ответ на определение, что платежная транзакция была инициирована с использованием мобильного устройства, аутентифицируют потребителя.

Другие цели и преимущества вариантов воплощения настоящего изобретения будут очевидны для специалиста в данной области техники после обзора подробного описания настоящего изобретения и приложенных фигур.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Фиг. 1 - схема, иллюстрирующая поток данных между различными компонентами системы аутентификации, которая может использоваться во время процесса регистрации для мобильного платежного устройства, в соответствии с некоторыми вариантами воплощения настоящего изобретения;

Фиг. 2 - схема, иллюстрирующая поток данных между различными компонентами процесса одобрения транзакции, который может использоваться во время платежной транзакции, выполняемой с использованием мобильного платежного устройства, в соответствии с некоторыми вариантами воплощения настоящего изобретения;

Фиг. 3 - схема, иллюстрирующая поток данных между различными компонентами системы аутентификации, которая может использоваться во время процесса регистрации для мобильного платежного устройства и специфических для мобильного устройства данных аутентификации, в соответствии с некоторыми вариантами воплощения настоящего изобретения;

Фиг. 4 - схема, иллюстрирующая поток данных между различными компонентами процесса одобрения транзакции, который может использоваться во время платежной транзакции, выполняемой с использованием мобильного платежного устройства и специфического мобильного пароля, в соответствии с некоторыми вариантами воплощения настоящего изобретения;

Фиг. 5 - функциональная блок-схема элементов мобильного платежного устройства в виде мобильного телефона, который может использоваться с некоторыми вариантами воплощения настоящего изобретения; и

Фиг. 6 - функциональная блок-схема вычислительной системы, устройства или прибора, которые могут использоваться для реализации некоторых процессов или операций, которые являются частью вариантов воплощения настоящего изобретения.

ПОДРОБНОЕ ОПИСАНИЕ

Варианты воплощения изобретения направлены на системы, устройства и способы для обеспечения возможности аутентификации транзакции или участника для транзакции в ситуации, в которой участник является удаленным от другой стороны для транзакции. Примером такой ситуации является транзакция без наличия карты (или более точно, без наличия платежного устройства), например, проводимая с использованием мобильного платежного устройства. Изобретение включает в себя инфраструктуру и процессы для обеспечения потребителю возможности зарегистрировать свой номер мобильного телефона и связать этот номер с платежным счетом. Процесс регистрации может быть выполнен с использованием веб-сайта, и регистрация может потребовать, чтобы потребитель обеспечил данные аутентификации, которые были предварительно предоставлены потребителем и связаны с платежным счетом. Таким образом, номер мобильного телефона потребителя становится связанным с платежным счетом аутентифицированным способом. После регистрации потребитель может использовать свой мобильный телефон для инициирования или выполнения одного или более этапов платежной транзакции. Платежная транзакция распознается как инициированная или выполненная посредством мобильного телефона, и в ответ сервер может аутентифицировать транзакцию на основе номера мобильного телефона и результата предшествующего процесса регистрации и аутентификации. В других вариантах воплощения сервер может распознать платежную транзакцию как инициированную или выполненную посредством мобильного телефона, и в ответ связывается с потребителем с использованием мобильного телефона, чтобы запросить подтверждение желания потребителя выполнить транзакцию. В качестве примеров это подтверждение может принять форму ответа на вызов на мобильный телефон, сформированный посредством интерактивной речевой системы (IVR) или посредством потребителя, обеспечивающего дополнительные данные аутентификации, которые были предварительно предоставлены потребителем и связаны с мобильным телефоном (с пониманием того, что дополнительные данные аутентификации могут быть использованы потребителем для авторизации транзакций, выполняемых с использованием мобильного телефона).

Многие, если не все, системы, устройства и способы настоящего изобретения могут быть реализованы с использованием элементов инфраструктуры, которые теперь используются для аутентификации платежных устройств и участников в транзакциях с наличием карты. Таким образом, варианты воплощения настоящего изобретения могут позволить банкам и другим поставщикам услуг мобильных платежей усилить существующие платформы аутентификации для обеспечения услуг аутентификации для транзакций без наличия карты, инициируемых с использованием мобильных платежных

устройств. Это уменьшает стоимость обеспечения услуг мобильных платежей потребителям и может увеличить признание таких служб, поскольку потребители и другие объекты, вовлеченные в процесс платежных транзакций, уже будут знакомы со многими, если не всеми, используемыми системами и процессами. Кроме того, варианты воплощения настоящего изобретения могут использоваться потребителями и другими объектами, вовлеченными в платежную транзакцию, для обеспечения улучшенной безопасности (включающей в себя несколько уровней безопасности при аутентификации потребителя, проводящего транзакцию), увеличения скорости обработки транзакций и большего удобства для потребителей, чем это было возможно в отсутствие изобретения.

Перед описанием вариантов воплощения системы и способов изобретения будут представлены некоторые термины, сокращения и определения, которые используются для описания этих вариантов воплощения.

Используемый здесь в некоторых вариантах воплощения термин "эмитент" может относиться к любому подходящему объекту, который может открывать и поддерживать счет, связанный с потребителем. Примеры эмитента включают в себя банк, кредитный союз, предприятие, такое как розничный магазин или поставщик услуг, или правительственный объект. Во многих случаях эмитент может обеспечить потребителю карту электронной коммерции или другой вид платежного устройства. Эмитент обычно имеет установленные отношения с потребителем и, таким образом, имеет данные, которые могут использоваться для аутентификации потребителя. Такие данные могут включать в себя номер социального страхования потребителя, день рождения, номер счета, адрес доставки, предпочтения и т.д.

Используемый в данном описании в некоторых вариантах воплощения термин "сервер" обычно представляет мощный компьютер или кластер компьютеров. Например, сервер может представлять собой большой универсальный компьютер, кластер мини-компьютеров или группу серверов, функционирующих как блок. В одном примере сервер может являться сервером базы данных, соединенным с веб-сервером. Кроме того, сервер может вести себя как компьютер, который обслуживает запросы одного или более клиентских компьютеров или портативных электронных устройств.

Используемый в данном описании в некоторых вариантах воплощения термин "торговый сервер" представляет сервер, используемый для предоставления потребителям интерактивной электронной витрины, где потребители могут делать покупки и проводить интерактивные транзакции после того, как они решают купить у продавца товары или услуги.

Используемый в данном описании в некоторых вариантах воплощения термин "поставщик услуг мобильных платежей" (или "Оператор MPI" или "MPI") выполняет различные функции аутентификации от имени продавца. Поставщик услуг мобильных платежей может использовать подходящее аппаратное обеспечение и/или программное обеспечение, которое доступно для продавца, для обеспечения этих функций. Например, оператор MPI может использовать программное обеспечение, работающее на торговом сервере, или это может быть компонент, работающий на другом сервере, доступном для продавца. Среди прочих функций оператор MPI может определять, доступна ли аутентификация для карты или номера платежного счета, или проверять цифровую подпись в сообщении аутентификации. В некоторых вариантах воплощения поставщик услуг мобильных платежей может использовать компонент, который работает в домене обслуживающей стороны.

Используемый в данном описании в некоторых вариантах воплощения термин

"сервер управления доступом" (или "ACS") предоставляет эмитентам (или другим объектам, способным аутентифицировать потребителя, проводящего интерактивную транзакцию или транзакцию без наличия карты) возможность аутентифицировать потребителей во время транзакции. Сервер ACS выполняет запрашиваемые службы аутентификации и обеспечивает в цифровой форме подписанные ответы объектам, запрашивающим аутентификацию. Сервер ACS может совместно использоваться несколькими сторонами. В качестве альтернативы сторона может иметь несколько серверов управления доступом, каждый из которых связан с отдельным поднабором потребителей.

Используемый в данном описании в некоторых вариантах воплощения термин "сервер каталогов" может использоваться для маршрутизации сообщений, содержащих информацию регистрации и аутентификации, между торговым модулем или поставщиком услуг мобильных платежей и сервером ACS эмитента. Сервер каталогов также может определять, может ли потребитель использовать службы аутентификации. В некоторых вариантах воплощения сервером каталогов может управлять организация обработки или обслуживания платежей, такая как Visa.

Используемый в данном описании в некоторых вариантах воплощения термин "система обработки платежей" или "сеть обработки оплаты" может включать в себя серверные компьютеры обработки данных, подсистемы, сети и операции, используемые для поддержки и поставки служб авторизации, служб файла исключений и служб произведения расчетов и урегулирования счета. Примерная система или сеть обработки платежей могут включать в себя VisaNet. Системы и сети обработки платежей могут обрабатывать транзакции по кредитной карте, транзакции по дебетовой карте и коммерческие транзакции других типов. Системы и сети обработки платежей также могут иметь системы, которые выполняют службы произведения расчетов и урегулирования счета. Система или сеть обработки платежей может использовать любую подходящую проводную или беспроводную сеть, в том числе Интернет, чтобы разрешить связь и передачу данных между компонентами или элементами.

Используемый в данном описании в некоторых вариантах воплощения термин "интерактивная речевая система" (или "IVR") относится к технологии систем телефонии, которая позволяет компьютерному устройству обнаруживать речь и тоновый набор через обычный телефонный вызов и обеспечивать взаимодействие с потребителем посредством телефонного вызова.

Используемый в данном описании в некоторых вариантах воплощения термин "служба коротких сообщений" (или "SMS") может использоваться для обозначения известного протокола для сообщений, которые отправляют с мобильных телефонов и на мобильные телефоны. Типичные сообщения SMS могут позволить пользователям отправлять до 160 символов на одно сообщение.

Используемый в данном описании в некоторых вариантах воплощения термин "номер ISDN мобильного абонента" (или "MSISDN") может использоваться для обозначения номера мобильного абонента в цифровой сети связи с интегрированным обслуживанием (ISDN), который может являться номером мобильного телефона потребителя.

Как отмечено выше, варианты воплощения изобретения могут быть особенно полезными для проведения удаленных транзакций, то есть в случае, когда потребитель и платежное устройство не присутствуют у продавца. Удаленные транзакции могут быть проведены через способы связи, в том числе, но без ограничения, голосовые вызовы мобильной или наземной связи, сообщения службы коротких сообщений (SMS)

и т.д. Различные протоколы передачи данных (например, TCP/IP) также могут использоваться. Удаленные транзакции могут быть инициированы с мобильных платежных устройств, в том числе, но без ограничения, мобильных телефонов, смартфонов, соединенных с Интернетом компьютеров или терминалов, карманных компьютеров (PDA) и т.д.

В некоторых вариантах воплощения, перед обеспечением возможности потребителю использовать свое мобильное платежное устройство для платежной транзакции мобильное устройство регистрируется и связывается с платежным счетом, принадлежащим потребителю. Процесс регистрации может включать в себя процесс аутентификации, в котором у потребителя требуют предоставить информацию, которая подтверждает его идентификационную информацию или доказывает, что он авторизован для проведения платежных транзакций с использованием платежного счета. Такая информация может принять форму кодового слова, пароля, данных безопасности или другого вида данных аутентификации или идентификации, которые предварительно были предоставлены службе аутентификации. В таком случае информация для потребителей была предварительно проверена и установлена в качестве удовлетворительного способа "доказательства", что человек, предоставляющий информацию, является потребителем, который авторизован для использования платежного счета. Например, у потребителя, стремящегося зарегистрировать свое мобильное платежное устройство, можно попросить предоставить его номер мобильного телефона или другой вид идентификатора мобильного платежного устройства и номер счета для платежного счета, который он хочет связать с мобильным идентификатором. Служба аутентификации затем может запросить, чтобы потребитель предоставил форму данных аутентификации для подтверждения своей идентификационной информации (например, пароль и т.д.), причем данные аутентификации были предварительно предоставлены и связаны с потребителем. Если данные аутентификации, предоставленные потребителем, проверены и являются корректным (то есть они являются данными, предварительно предоставленными и связанными с потребителем или платежным счетом потребителя), то идентификатор мобильного устройства связывается с платежным счетом потребителя. Как будет описано, в некоторых вариантах воплощения изобретения это может обеспечить потребителю возможность выполнять платежные транзакции с использованием мобильного устройства без необходимости предоставлять дополнительные данные аутентификации или идентификации.

Таким образом, в некоторых вариантах воплощения изобретения потребитель может быть аутентифицирован (например, в целях проведения транзакции в более позднее время), в то время как потребитель находится в процессе регистрации в службе мобильных платежей. Потребитель затем может провести транзакции с использованием службы мобильных платежей без необходимости дополнительной аутентификации во время транзакции. Это предоставляет потребителю удобный способ использовать свое мобильное платежное устройство для платежных транзакций.

Как отмечено, некоторые аспекты процесса аутентификации потребителя могут быть сделаны во время регистрации мобильного платежного устройства в качестве гарантии, что только потребитель, который должным образом аутентифицирован службой аутентификации, может зарегистрироваться в службе мобильных платежей (и, таким образом, использовать свое мобильное платежное устройство для выполнения платежных транзакций). В качестве примера потребитель может зарегистрироваться в службе мобильных платежей посредством регистрации номера мобильного телефона

и персонального номера счета (PAN) у поставщика услуг мобильных платежей. В некоторых вариантах воплощения сервер ACS может попросить потребителя предоставить предварительно принятый пароль, который был связан с платежным счетом. В некоторых вариантах воплощения сервер ACS может решить аутентифицировать потребителя через отдельный канал или запрос как часть процесса регистрации (например, посредством вызова по мобильному телефону, отправки запроса информацию через службу обмена сообщениями на настольный компьютер и т.д.). Во время последующей транзакции, инициируемой потребителем, поставщик услуг мобильных платежей может проверить телефонный номер и номер PAN, используемые потребителем во время транзакции. В некоторых вариантах воплощения во время транзакции поставщик услуг мобильных платежей может запросить создание подписи аутентификации у сервера ACS без прохождения через отдельный процесс аутентификации с потребителем.

Следует отметить, что в некоторых вариантах воплощения поставщик услуг мобильных платежей и оператор ACS в домене эмитента могут войти в двустороннее соглашение, чтобы гарантировать, что система ACS может отличить транзакцию, проводимую на мобильном канале, и транзакцию на основе веб-сети. Как будет описано, это может быть сделано, чтобы обеспечить системе изобретения возможность распознавать, что транзакция проводится с использованием мобильного платежного устройства и в ответ применять заданный процесс авторизации к этой транзакции. Следует отметить, что при желании поставщик услуги мобильных платежей может изменить свою систему регистрации в службе, чтобы гарантировать, что в службе мобильных платежей могут зарегистрироваться только те пользователи, которые аутентифицированы указанной системой аутентификации. В других вариантах воплощения система ACS может быть выполнена с возможностью быть в состоянии отличать и аутентифицировать мобильную транзакцию без какого-либо соглашения, участия или изменения посредством поставщика услуг мобильных платежей. Учитывая большое количество продавцов электронной коммерции, возможность аутентифицировать транзакции мобильного платежа без требования изменений посредством продавца может быть полезной. В таких вариантах воплощения, когда потребитель перенаправляется продавцом на сервер ACS, сервер ACS использует HTTP-заголовки, чтобы распознать, что потребитель использует мобильное устройство. Затем сервер ACS отправляет должным образом сформатированное окно запроса пароля потребительскому устройству. Потребитель вводит свой предварительно зарегистрированный пароль, сервер ACS аутентифицирует потребителя и предоставляет результаты аутентификации обратно поставщику услуг мобильных платежей.

Фиг. 1 является схемой, иллюстрирующей поток данных между различными компонентами системы аутентификации, которая может использоваться во время процесса регистрации для мобильного платежного устройства, в соответствии с некоторыми вариантами воплощения настоящего изобретения. Как показано на фиг. 1, в типичном варианте использования пользователь или потребитель 1000 использует клиент 1100, такой как веб-браузер, работающий на персональном компьютере, чтобы зарегистрировать мобильное платежное устройство для использования с платежным счетом. Потребитель 1000 регистрирует свой персональный номер счета (PAN) и номер MSISDN посредством отправки этой информации оператору 1200 MPI через клиент 1100. Как правило, номер MSISDN будет являться номером мобильного телефона потребителя в случае мобильного платежного устройства, представляющего собой мобильный телефон; однако если платежное устройство не является мобильным

телефоном, то номер MSISDN может представлять собой другой вид данных. В некоторых вариантах воплощения потребитель 1000 использует веб-браузер, работающий на клиенте 1100, для осуществления доступа к веб-сайту, исполняемому посредством оператора 1200 MPI, чтобы предоставить эту информацию. Следует отметить, что клиент 1100 может не являться устройством мобильной связи, которое регистрируется потребителем 1000 для использования в качестве мобильного платежного устройства, хотя в некоторых вариантах воплощения клиент может представлять собой то же самое устройство (или резидентный объект на устройстве), которое регистрируется как мобильное платежное устройство. Предоставление этой информации показано как поток 110 данных на фиг. 1.

Затем оператор 1200 MPI определяет надлежащий сервер 1300 ACS для заданного платежного счета, предоставленного потребителем 1000. В некоторых вариантах воплощения оператор 1200 MPI осуществляет доступ к серверу каталогов для поиска надлежащего сервера 1300 ACS. Как только оператор 1200 MPI определил местоположение надлежащего сервера 1300 ACS, оператор 1200 MPI отправляет номер PAN с номером MSISDN, предоставленные потребителем 1000 серверу 1300 ACS. Передача номера PAN и номера MSISDN показана как поток 120 данных на фиг. 1.

Сервер 1300 ACS может затем взаимодействовать с клиентом 1100, используемым потребителем 1000, для выполнения или завершения процесса регистрации. Следует отметить, что в некоторых вариантах воплощения процесс регистрации может включать в себя часть или все процессы аутентификации. В некоторых вариантах воплощения регистрация может включать в себя отправку сервером 1300 ACS веб-страницы клиенту 1100 по Интернету. Передача веб-страницы показана как поток 130 данных. Потребитель 1000 может затем ввести пароль или другие данные безопасности на веб-странице и предоставить эту информацию обратно серверу 1300 ACS. Пароль или другие данные безопасности, предоставленные потребителем, могут представлять собой пароль или данные, которые были предварительно установлены потребителем 1000, для аутентификации транзакций без наличия карты, таких как транзакции, проводимые на сайтах электронной коммерции по Интернету (хотя это не требуется, поскольку пароль или данные могли быть установлены потребителем для аутентификации других типов платежных транзакций). Таким образом, в некоторых вариантах воплощения потребитель может зарегистрировать свою информацию о платежном счете и предоставить пароль, который будет использоваться для аутентификации потребителя в некоторых ситуациях транзакций. Когда потребитель позже хочет зарегистрировать свой номер мобильного телефона и номер PAN, чтобы использовать свой мобильный телефон для транзакций мобильного платежа, его можно попросить обеспечить предварительно предоставленный пароль для его аутентификации. Ответ потребителя может также служить для подтверждения его желания иметь номер мобильного телефона, связанный с номером PAN, в целях использования своего мобильного телефона для платежных транзакций. Следует отметить, что в некоторых вариантах воплощения пароль, предоставленный серверу 1300 ACS, может быть новым паролем, который регистрируется потребителем для использования с транзакциями без наличия карты или более определенно для мобильных транзакций. Предоставление пароля серверу 1300 ACS показано как поток 140 данных.

Если предоставленный пароль является тем, который был предварительно установлен потребителем, то сервер 1300 ACS может подтвердить пароль и отправить результат аутентификации (то есть, что потребитель должным образом аутентифицирован) оператору 1200 MPI. Сервер 1300 ACS также может отправить другую информацию с

результатом аутентификации, такую как значение проверки аутентификации владельца кредитной карты (CAVV). Это взаимодействие показано как поток 150 данных. Предварительно установленный пароль может быть таким, как описано в патенте США № 7,007,840, который описывает процесс для предоставления потребителю возможности зарегистрировать номер PAN, соответствующий потребительскому платежному счету, и связать этот счет с паролем, который потребитель может использовать в более позднее время для своей аутентификации. Если предоставленный пароль является новым паролем, который регистрируется потребителем, то сервер 1300 ACS может запросить от потребителя другие данные, прежде чем предоставить оператору 1200 MPI показание, что потребитель аутентифицирован. Такие другие данные могут включать в себя, например, потребительский профиль или идентификационные данные.

После приема подтверждения, что потребитель аутентифицирован, оператор 1200 MPI может отправить сообщение аутентификации эмитенту 1500 для проверки предоставленного значения (CVV2) проверки карты и подтвердить, что платежный счет, который потребитель хочет использовать для транзакции с помощью мобильного платежного устройства, является активным. Оператор 1200 MPI может предоставить это сообщение аутентификации эмитенту 1500 с использованием системы 1400 обработки платежей. Этот поток данных показан как 160 и 170. Когда платежный счет (например, кредитная или дебетовая карта) проверен, мобильное платежное устройство регистрируется для использования потребителем 1000 в транзакциях без наличия карты.

Фиг. 2 является схемой, иллюстрирующей поток данных между различными компонентами процесса одобрения транзакции, который может использоваться во время платежной транзакции, выполняемой с использованием мобильного платежного устройства, в соответствии с некоторыми вариантами воплощения настоящего изобретения. Как показано на фигуре, в типичной платежной транзакции потребитель 1000 инициирует транзакцию без наличия карты с использованием зарегистрированного мобильного платежного устройства 2100 потребителя 1000 (когда процесс регистрации проводится в соответствии с процессом, изображенным на фиг. 1, или в другом подходящем процессе). В некоторых вариантах воплощения потребитель 1000 может инициировать транзакцию посредством ввода клиентского PIN (персонального идентификационного номера) в мобильное платежное устройство 2100, посредством активации платежного приложения, установленного на мобильном устройстве 2100, посредством обеспечения другого вида управления доступом или данных безопасности устройству или посредством участия в другом виде взаимодействия пользователя с устройством. В ответ мобильное платежное устройство 2100 затем инициирует платежную транзакцию с узлом 1200 оператора мобильных платежей. Этот этап показан как поток 210 данных. Данные, переданные в потоке 210 данных, могут включать в себя номер MSISDN мобильного платежного устройства, хотя они также могут включать в себя другие данные в дополнение к номеру MSISDN или вместо него.

На основе номера MSISDN и/или других данных, принятых от мобильного платежного устройства 2100, оператор 1200 MPI может определить потребительский платежный счет, связанный с потребителем. Оператор 1200 MPI поставщика услуг мобильных платежей может затем запросить аутентификацию от сервера ACS 1300, связанного с платежным счетом зарегистрированного мобильного платежного устройства 2100 (или, более точно, подтверждение предыдущей аутентификации потребителя и/или мобильного платежного устройства). В некоторых вариантах воплощения оператор 1200 MPI может использовать сервер каталогов для поиска надлежащего сервера 1300 ACS для

платежного счета потребителя 1000. Когда оператор 1200 MPI определил надлежащий сервер 1300 ACS для аутентификации, оператор 1200 MPI может отправить запрос аутентификации серверу 1300 ACS. Этот запрос оператора 1200 MPI к серверу ACS 1300 показан как поток 220 данных.

Сервер 1300 ACS распознает запрос от оператора 1200 MPI как связанный с транзакцией мобильного платежа, инициированной с использованием заданного мобильного платежного устройства, и на основе данных, предоставленных как часть предыдущей регистрации и процесса аутентификации (как описано в отношении фиг. 1), может создать сообщение одобрения аутентификации или транзакции для платежной транзакции. Согласно некоторым вариантам воплощения сервер 1300 ACS, необязательно, может заставить сформировать вызов IVR на мобильное платежное устройство 2100 для подтверждения намерения потребителя 1000 провести транзакцию. Необязательный вызов IVR показан как поток 230 и 240 данных, где один элемент потока данных представляет собой сформированный вызов IVR на мобильное устройство, и другой элемент потока данных представляет собой ответ на вызов IVR, сформированный потребителем, использующим мобильное устройство. После выполнения любых дополнительных операций аутентификации или проверки, которые могут быть использованы (или без выполнения подобных операций, если они не требуются), сервер 1300 ACS отправляет результат аутентификации оператору 1200 MPI, причем это показано как поток 250 данных. Результат аутентификации может содержать другие соответствующие данные аутентификации, такие как CAVV. Следует отметить, что в дополнение к использованию системы IVR также могут быть использованы другие формы подтверждения намерения потребителя провести транзакцию; они включают в себя, но без ограничения, обмен сообщениями SMS, электронными письмами, обеспечение потребителем заданного числового или алфавитно-цифрового кода в ответ на сообщение и т.д. Следует также отметить, что использование вызова IVR или другой формы подтверждения намерения потребителя провести транзакцию может применяться выборочно только к некоторым транзакциям, таким как транзакции, подозрительные на предмет мошенничества, транзакции, имеющие значение, которое превышает предопределенную пороговую величину, или по любым другим подходящим критериям.

Оператор 1200 MPI использует результат аутентификации, принятый от сервера 1300 ACS (который, как отмечено, может включать в себя такие данные, как CAVV и/или другие данные, относящиеся к платежному устройству или платежному счету), для обеспечения авторизации для платежной транзакции эмитенту 1500 для платежного счета, используемого потребителем. Эта авторизация может быть передана через систему 1400 обработки платежей, причем процесс показан как потоки 260 и 270 данных. Авторизация, переданная эмитенту, может включать в себя информацию, которая идентифицирует транзакцию как транзакцию без наличия карты, проводимую с использованием авторизованного мобильного платежного устройства.

Следует отметить, что в примерном процессе платежной транзакции, описанном в отношении фиг. 2, никакая дополнительная аутентификация потребителя не требуется для выполнения сервером 1300 ACS во время транзакции (хотя, как отмечено, может быть использована аутентификация IVR или другой вид дополнительной аутентификации). Вместо этого сервер 1300 ACS распознает транзакцию, принятую от оператора 1200 MPI, как транзакцию без наличия карты, которая инициирована с использованием предварительно аутентифицированного мобильного платежного устройства 2100. Это позволяет потребителю провести платежную транзакцию с

помощью мобильного платежного устройства без необходимости предоставлять дополнительную информацию аутентификации, тем самым уменьшая неудобство для потребителя и ускоряя транзакцию.

В качестве альтернативы для варианта воплощения изобретения, описанного в отношении фиг. 1 и 2, в некоторых вариантах воплощения во время процесса регистрации потребитель может обеспечить пароль или другой вид данных аутентификации, которые должны использоваться специально для авторизации платежной транзакции, инициируемой с использованием мобильного платежного устройства, или заданного мобильного платежного устройства. В таком варианте воплощения потребитель регистрирует свое мобильное платежное устройство способом, аналогичным описанному в отношении фиг. 1; однако во время процесса регистрации потребитель предоставляет серверу аутентификации пароль или другой вид данных аутентификации, которые зарегистрированы и связаны с транзакциями, которые выполняются с использованием мобильного платежного устройства потребителя. Во время последующей платежной транзакции, которая инициируется с использованием мобильного платежного устройства, у потребителя запрашивается предоставление зарегистрированных данных аутентификации, которые были связаны с устройством в виде аутентификации потребителя и одобрения транзакции.

Таким образом, в этом альтернативном варианте воплощения потребителя можно попросить обеспечить новый числовой пароль (или данные другой подходящей формы, такие как алфавитно-цифровой пароль или строка символов) для использования с мобильным платежным устройством потребителя, когда потребитель регистрирует свое мобильное платежное устройство для использования в платежных транзакциях. После регистрации в службе мобильных платежей потребитель может выполнить платежную транзакцию с использованием своего мобильного устройства, причем транзакция аутентифицируется с использованием числового пароля или других данных. Новый пароль может быть (и в некоторых случаях желательно быть) отличающимся от других паролей, которые могут использоваться для аутентификации пользователя для других типов транзакций, таких как транзакции электронной коммерции, проводимые по Интернету. Таким образом, альтернативный вариант воплощения позволяет потребителю создавать и регистрировать на сервере ASC пароль, специализированный для мобильного платежного устройства. Потребитель вводит выделенный пароль в мобильное платежное устройство, такое как мобильный телефон, при проведении транзакции с использованием мобильного платежного устройства. Затем пароль может быть направлен от мобильного устройства через оператора мобильного платежа на сервер ACS для аутентификации потребителя и одобрения транзакции.

Следует отметить, что в некоторых реализациях варианты воплощения процесса изобретения могут потребовать, чтобы изменения были произведены в пределах домена поставщика услуг мобильных платежей (который может являться частью торгового домена) и/или на сервере ACS (который может являться частью домена эмитента) для системы аутентификации, которая выполнена с возможностью аутентифицировать стандартные транзакции электронной коммерции (то есть транзакции, не выполняемые с использованием мобильного платежного устройства). Реализация вариантов воплощения изобретения также может привести к реконфигурации торгового модуля в торговом домене и/или модификации в домене эмитента (то есть на сервере ACS) для размещения процесса аутентификации на основе мобильных платежных устройств. Кроме того, в некоторых случаях поставщику услуг мобильных платежей может

потребоваться реализовать модификации для своего узла и клиентского программного обеспечения мобильного телефона для поддержки ввода мобильного пароля потребителем для каждой транзакции и направления пароля оператору сервера ACS.

Далее со ссылкой на фиг. 3 будет описан альтернативный вариант воплощения настоящего изобретения, в котором специфический для мобильного платежного устройства пароль или данные аутентификации используются для платежных транзакций, инициируемых с использованием мобильного платежного устройства. Фиг. 3 является схемой, иллюстрирующей поток данных между различными компонентами системы аутентификации, которая может использоваться во время процесса регистрации для мобильного платежного устройства и специфических для мобильного устройства данных аутентификации в соответствии с некоторыми вариантами воплощения настоящего изобретения.

Как показано на фигуре, потребитель 1000 использует клиент 1100, такой как веб-браузер, работающий на персональном компьютере, для регистрации мобильного платежного устройства для использования с платежным счетом. Потребитель 1000 регистрирует свой персональный номер счета (PAN) и номер MSISDN посредством отправки этой информации оператору 1200 MPI через клиент 1100. Как правило, номер MSISDN будет являться номером мобильного телефона потребителя в случае мобильного платежного устройства, представляющего собой мобильный телефон; однако если платежное устройство не является мобильным телефоном, то номер MSISDN может представлять собой другой вид данных. В некоторых вариантах воплощения потребитель 1000 использует веб-браузер, работающий на клиенте 1100, для осуществления доступа к веб-сайту, исполняемому посредством оператора 1200 MPI, чтобы предоставить эту информацию. Следует отметить, что клиент 1100 может не являться устройством мобильной связи, которое регистрируется потребителем 1000 для использования в качестве мобильного платежного устройства, хотя в некоторых вариантах воплощения клиент может представлять собой то же самое устройство (или резидентный объект на устройстве), которое регистрируется как мобильное платежное устройство. Предоставление этой информации показано как поток 310 данных на фиг. 3.

Затем оператор 1200 MPI определяет надлежащий сервер 1300 ACS для платежного счета, соответствующего данным, предоставленным потребителем 1000. Согласно одному варианту воплощения оператор 1200 MPI осуществляет доступ к серверу каталогов для поиска надлежащего сервера 1300 ACS. Когда оператор 1200 MPI определил местоположение надлежащего сервера 1300 ACS, оператор 1200 MPI может отправить номер PAN с номером MSISDN, предоставленным потребителем 1000, серверу 1300 ACS. Передача номера PAN и номера MSISDN показана как поток 320 данных на фиг. 3.

Сервер 1300 ACS может затем взаимодействовать с клиентом 1100, используемым потребителем 1000, для регистрации специфического для мобильного платежного устройства или специфического для мобильных транзакций пароля или другого вида данных аутентификации. Согласно одному варианту воплощения этот процесс начинается, когда сервер 1300 ACS отправляет клиенту 1100 веб-страницу по Интернету. Передача веб-страницы показана как поток 330 данных. Потребитель 1000 может затем ввести свой "стандартный" пароль на веб-сайте, а также новый специфический для мобильного платежного устройства или мобильных транзакций пароль и предоставить эту информацию обратно серверу 1300 ACS. Стандартный пароль, введенный потребителем, может являться паролем, который был предварительно установлен

потребителем 1000 для аутентификации транзакций без наличия карты, таких как транзакции, проводимые на сайтах электронной коммерции по Интернету (хотя это не требуется, поскольку пароль или данные могли быть установлены потребителем для аутентификации платежных транзакций других типов). Стандартный пароль может быть установлен посредством любого подходящего процесса или операции, например, как описано в отношении фиг. 1 или как описано в предварительно упомянутом патенте США № 7,007,840, озаглавленном "Управляемая активация владельцев кредитных карт в безопасной программе аутентификации", содержание которого включено в настоящий документ по ссылке во всей своей полноте для всех целей. Специфический для мобильного платежного устройства или мобильных транзакций пароль может быть числовым, алфавитно-цифровым или являться другим видом пароля или данных аутентификации, которые будут связаны с зарегистрированным мобильным платежным устройством и использованы в качестве части процесса аутентификации для транзакций без наличия карты, проводимых с использованием устройства. Предоставление этих паролей серверу 1300 ACS показано как поток 340 данных. Следует отметить, что стандартный пароль и специфический мобильный пароль могут быть предоставлены как часть одного и того же предоставления данных или как отдельные предоставления данных, например, с использованием двух отдельных форм на веб-страницах (причем предоставление специфического мобильного пароля может происходить в ответ на запрос или форму, сформированную в ответ на предоставление стандартного пароля).

Сервер 1300 ACS принимает предоставленные данные и может затем проверить стандартный пароль, установить специфический мобильный пароль для мобильного платежного устройства и отправить результат аутентификации оператору 1200 MPI. Сервер ACS 1300 может также отправить другую информацию с результатом аутентификации, такую как значение проверки аутентификации владельца кредитной карты (CAVV). Это взаимодействие показано как поток 350 данных.

Оператор 1200 может затем отправить сообщение аутентификации эмитенту 1500, чтобы проверить предоставленное значение (CVV2) проверки карты и подтвердить, является ли счет потребителя активным. Оператор 1200 MPI может предоставить это сообщение аутентификации эмитенту 1500 с использованием системы 1400 обработки платежей. Этот поток данных показан в качестве элементов 360 и 370 на фигуре. Когда карта проверена, мобильное платежное устройство регистрируется для использования потребителем 1000 в транзакциях без наличия карты.

Фиг. 4 является схемой, иллюстрирующей поток данных между различными компонентами процесса одобрения транзакции, который может использоваться во время платежной транзакции, выполняемой с использованием мобильного платежного устройства и специфического мобильного пароля в соответствии с некоторыми вариантами воплощения настоящего изобретения. В типичной платежной транзакции потребитель 1000 инициирует транзакцию без наличия карты с использованием зарегистрированного мобильного платежного устройства 2100 потребителя. В некоторых вариантах воплощения потребитель 1000 может инициировать транзакцию посредством ввода клиентского PIN (персонального идентификационного номера) в мобильное платежное устройство 2100, посредством активации платежного приложения, установленного на мобильном устройстве 2100, посредством обеспечения другого вида управления доступом или данных безопасности устройству или посредством участия в другом виде взаимодействия пользователя с устройством. В ответ мобильное платежное устройство 2100 инициирует платежную транзакцию с оператором 1200 службы мобильных платежей. Этот этап показан как поток 410 данных. Данные,

переданные в потоке 410 данных, могут включать в себя номер MSISDN мобильного платежного устройства, хотя они также могут включать в себя другие данные в дополнение к номеру MSISDN или вместо него.

На основе номера MSISDN и/или других данных, принятых от мобильного платежного устройства 2100, оператор 1200 MPI может определить потребительский платежный счет, связанный с потребителем. Затем оператор 1200 просит потребителя 1000 ввести или иным образом предоставить специфический для мобильного платежного устройства или для мобильных транзакций пароль, установленный во время процесса регистрации. В ответ потребитель 1000 вводит свой специфический мобильный пароль в мобильное платежное устройство 2100 и отправляет этот пароль обратно оператору 1200 MPI. Этот поток данных между мобильным платежным устройством 2100 и оператором 1200 MPI показан как потоки 420 и 430 данных на фигуре.

Оператор 1200 MPI затем отправляет запрос аутентификации серверу 1300 ACS. В некоторых вариантах воплощения оператор 1200 MPI может использовать сервер каталогов для поиска надлежащего сервера 1300 ACS для платежного счета потребителя 1000. Когда оператор 1200 MPI определил местоположение надлежащего сервера 1300 ACS, оператор 1200 MPI может отправить запрос аутентификации серверу 1300 ACS. Запрос аутентификации включает в себя специфический мобильный пароль, введенный потребителем 1000. Этот запрос аутентификации показан как поток 440 данных.

В некоторых вариантах воплощения сервер 1300 распознает, что запрос аутентификации, сделанный оператором 1200 MPI, выполнен для транзакции мобильного платежа без наличия карты, и сервер 1300 ACS поддерживает отдельный процесс аутентификации, который использует специфический мобильный пароль для мобильного платежного устройства 2100 для аутентификации потребителя (а не стандартный пароль или другой пароль для платежного счета). Сервер 1300 ACS аутентифицирует запрос на основе предоставления корректного специфического мобильного пароля и отправляет результат аутентификации оператору 1200. В некоторых вариантах воплощения результат аутентификации может включать в себя другие соответствующие данные аутентификации, такие как CAVV. Передача результата аутентификации оператору 1200 MPI показана как поток данных 450.

Согласно некоторым вариантам воплощения сервер 1300 ACS, необязательно, может заставить сформировать вызов IVR на мобильное платежное устройство 2100 для подтверждения намерения потребителя 1000 провести транзакцию. Вызов IVR может включать в себя сформированный вызов IVR на мобильное устройство и ответ на вызов IVR, сформированный потребителем, использующим мобильное устройство. Следует отметить, что в дополнение к использованию системы IVR также могут быть использованы другие формы подтверждения намерения потребителя провести транзакцию; они включают в себя, но без ограничения, обмен сообщениями SMS, электронными письмами, обеспечение потребителем заданного числового или алфавитно-цифрового кода в ответ на сообщение и т.д. Следует также отметить, что использование вызова IVR или другой формы подтверждения намерения потребителя провести транзакцию может применяться выборочно только к некоторым транзакциям, таким как транзакции, подозрительные на предмет мошенничества, транзакции, имеющие значение, которое превышает предопределенную пороговую величину, или по любым другим подходящим критериям.

Оператор 1200 MPI затем использует ответ аутентификации, принятый от сервера 1300 ACS, для авторизации транзакции без наличия карты с помощью эмитента 1500 платежного счета, используемого потребителем 1000. Оператор 1200 MPI может сделать

этот запрос с использованием системы обработки платежей. Это показано как потоки 460 и 470 данных на фигуре. Как проиллюстрировано на фиг. 4, специфический мобильный пароль направлен от потребителя 1000 к серверу 1300 ACS через оператора 1200 MPI.

Способы, процессы или операции, описанные со ссылкой на фиг. 1-4, могут быть осуществлены с использованием любого подходящего вида мобильного платежного устройства или портативного потребительского устройства, в том числе, но без ограничения, мобильного телефона, карманного компьютера (PDA), портативного компьютера или другого устройства, имеющего возможность беспроводной связи и передачи данных. Мобильное платежное устройство или портативное потребительское устройство могут включать в себя бесконтактный элемент, такой как полупроводниковую микросхему, встроенную или иным образом присоединенную к мобильному телефону, карманному компьютеру (PDA) и т.д. Как описано, в некоторых вариантах воплощения потребитель может использовать мобильное платежное устройство или портативное потребительское устройство, такое как мобильный телефон, для проведения платежных транзакций посредством обеспечения платежных данных и функционирования в качестве интерфейса для обеспечения данных аутентификации. Следует отметить, что варианты воплощения изобретения не ограничены каким-либо определенным типом мобильного платежного устройства или портативного потребительского устройства.

Примерное портативное потребительское устройство или мобильное платежное устройство могут находиться в одной из многих подходящих форм. Например, подходящие портативные мобильные платежные устройства могут быть переносными и компактными, с тем чтобы они могли помещаться в карман потребителя (например, карманными). Они могут включать в себя интеллектуальные микросхемы, встроенные в другое устройство. Примеры портативных потребительских устройств, которые могут функционировать в качестве платежных устройств, включают в себя сотовые телефоны, карманные компьютеры (PDA), пейджеры, транспондеры и т.п. Портативные потребительские устройства могут функционировать в качестве дебетовых устройств (например, дебетовой карты), кредитных устройств (например, кредитной карты) или устройств с предоплатой (например, карты с предоплатой).

Примерное мобильное платежное устройство может содержать считываемый компьютером носитель и корпус, как показано на фиг. 5, которая является функциональной блок-схемой элементов мобильного платежного устройства в виде мобильного телефона, который может использоваться с некоторыми вариантами воплощения настоящего изобретения. Следует отметить, что фиг. 5 показывает несколько компонентов, и портативные потребительские устройства или мобильные платежные устройства, используемые в качестве части реализации изобретения, могут содержать любую подходящую комбинацию или поднабор таких компонентов. Считываемый компьютером носитель (CRM) 32(b) может находиться в пределах корпуса 32(h) или может отделяться от этого. Корпус 32(h) может быть выполнен в виде пластмассовой подложки, кожуха или другой подходящей структуры. Считываемый компьютером носитель 32(b) может представлять собой память, которая хранит данные, и может быть выполнен в любой подходящей форме, в том числе магнитной полоски или микросхемы памяти, и может содержать уникально полученные ключи, алгоритмы шифрования и т.д. Память также может хранить такую информацию, как финансовая информация, информация транзакции (например, как в билетах для прохода в метро или на железнодорожный транспорт), информация доступа (например, как в пропусках)

и т.д. Финансовая информация может включать в себя такую информацию, как информация банковского счета, идентификационный номер банка (BIN), информация номера кредитной или дебетовой карты, информация баланса счета, дата истечения срока, информация о потребителе, такая как имя, дата рождения и т.д.

Информация в памяти также может быть в виде дорожек данных, таких как традиционно относящиеся к кредитным картам. Такие дорожки могут включать в себя дорожку 1 и дорожку 2. Дорожка 1 обычно хранит больше информации, чем дорожка 2, и содержит имя владельца кредитной карты, а также номер счета и другие произвольные данные. Эта дорожка иногда используется авиалиниями при защите резервирований с помощью кредитной карты. Дорожка 2 в настоящий момент обычно используется для платежных транзакций. Это дорожка, которая считывается банкоматами (ATM) и терминалами приема кредитных карт. Дорожка обычно содержит счет владельца кредитной карты, зашифрованный PIN-код и другие произвольные данные.

Считываемый компьютером носитель 32(b) или память может содержать код, который при его исполнении посредством запрограммированного процессора вызывает реализацию соответствующих этапов, процессов или операций настоящего изобретения. Например, считываемый компьютером носитель 32(b) может содержать код, который при его исполнении помогает при регистрации мобильного платежного устройства и при использовании мобильного платежного устройства в транзакции без наличия карты (CNP).

Телефон 32 может дополнительно включать в себя бесконтактный элемент 32(g), который может включать в себя полупроводниковую микросхему (или другой элемент хранения данных) и в некоторых вариантах воплощения соответствующий элемент беспроводной передачи данных, такой как антенна или преобразователь. Следует отметить, что элемент беспроводной передачи данных не требуется во всех вариантах воплощения изобретения, поскольку бесконтактный элемент может быть интегрирован с возможностями связи мобильного телефона, и тем самым разрешается передача данных между бесконтактным элементом и системой сотовой связи. В таких ситуациях бесконтактный элемент 32(g) может быть встроен в телефон 32, и данные или инструкции управления, переданные через сотовую связь, могут быть применены к бесконтактному элементу 32(g) посредством интерфейса бесконтактного элемента (не показан). Интерфейс бесконтактного элемента делает возможным обмен данными и/или инструкциями управления между схемой мобильного устройства (и, следовательно, сетью сотовой связи) и бесконтактным элементом 32(g).

В некоторых вариантах воплощения бесконтактный элемент 32(g) имеет возможность передачи и приема данных с использованием беспроводной связи ближнего радиуса действия (NFC) (или среды беспроводной связи ближнего радиуса действия) обычно в соответствии со стандартизированным протоколом или механизмом передачи данных (например, ISO 14443/NFC). Другие подходящие возможности связи малой дальности, которые могут использоваться для реализации изобретения, включают в себя RFID, Bluetooth™, инфракрасное излучение или другие возможности передачи данных, которые могут использоваться для обмена данными между телефоном 32 и считывающим устройством или терминалом точки продажи. Таким образом, телефон 32 может иметь возможность взаимодействия и передачи данных и/или инструкций управления как через сеть сотовой связи, так с использованием беспроводной связи ближнего радиуса действия или малой дальности.

Телефон 32 также будет обычно включать в себя процессор 32(c) (например,

микропроцессор или ЦП), запрограммированный с помощью набора инструкций, причем процессор исполняет инструкции для реализации различных функций телефона 32 и устройства 32(d) отображения, чтобы предоставить потребителю возможность видеть номера телефонов и другую информацию и сообщения. Телефон 32 может дополнительно включать в себя элементы 32(e) ввода (такие как клавиатура, экран касания и т.д.), чтобы предоставить потребителю (или представителю) возможность вводить информацию в устройство, динамик 32(f), чтобы предоставить потребителю возможность слышать голосовую связь, музыку и т.д., и микрофон 32(i), чтобы предоставить потребителю возможность вводить свою речь в телефон 32. Телефон 32 также будет обычно включать в себя антенну 32(a) для обеспечения возможности беспроводной связи и передачи данных с использованием сети сотовой связи.

Фиг. 6 является функциональной блок-схемой вычислительной системы, устройства или прибора, которые могут использоваться для реализации некоторых процессов или операций, которые являются частью вариантов воплощения настоящего изобретения. В примерном варианте воплощения некоторые или все функциональные компоненты, изображенные на фиг. 6, могут присутствовать на сервере или в другом виде вычислительного устройства, которое выполняет некоторые или все функции оператора MPI (элемент 1200 на фиг. 1-4), сервера ACS (элемент 1300 на фиг. 1-4) или системы обработки платежей (элемент 1400 на фиг. 1-4), которые описаны в отношении вариантов воплощения настоящего изобретения. Подсистемы, показанные на фиг. 6, соединены между собой через системную шину 675. Показаны дополнительные подсистемы, такие как принтер 674, клавиатура 678, жесткий диск 679 (или другая память, содержащая считываемые компьютером носители), монитор 676, который присоединен к адаптеру 682 устройства отображения, и другие. Периферийные устройства и устройства ввода/вывода, которые присоединены к контроллеру 671 ввода/вывода, могут быть соединены с компьютерной системой посредством любого количества средств, известных в данной области техники, таких как последовательный порт 677. Например, последовательный порт 677 или внешний интерфейс 681 могут использоваться для соединения вычислительного устройства с глобальной сетью, такой как Интернет, устройством мыши или сканером. Соединение через системную шину позволяет центральному процессору 673 взаимодействовать с каждой подсистемой и управлять выполнением инструкций из системной памяти 672 или жесткого диска 679, а также осуществлять обмен информацией между подсистемами. Системная память 672 и/или жесткий диск 679 могут воплотить считываемый компьютером носитель. Как упомянуто, некоторые или все эти элементы могут присутствовать в предварительно описанных приборах или устройствах. Например, предварительно описанный сервер каталогов или сервер управления доступом могут включать в себя один или больше компонентов, показанных на фиг. 6.

Считываемый компьютером носитель в соответствии с вариантом воплощения изобретения может содержать код или другой вид исполняемых инструкций для выполнения любой из функций, процессов или операций, описанных в отношении вариантов воплощения настоящего изобретения. Например, предварительно описанный оператор MPI может представлять собой вычислительное устройство, которое включает в себя процессор и содержит считываемый компьютером носитель, содержащий код, который при его исполнении посредством запрограммированного процессора выполняет аутентификацию потребителя для проведения транзакции на мобильном устройстве при регистрации мобильного устройства для использования в транзакциях, и код для проведения транзакции с использованием мобильного устройства. Таким образом,

оператор MPI может включать в себя процессор, присоединенный к считываемому компьютером носителю, причем процессор исполняет инструкции, воплощенные посредством компьютерного кода на считываемом компьютером носителе.

Примененные здесь термины и выражения используются в качестве терминов описания, а не ограничения, и при использовании таких терминов и выражений не имеется намерения исключения эквивалентов показанных и описанных признаков или их частей; признается, что в рамках объема заявленного изобретения возможны различные модификации. Кроме того, любой один или более признаков любого варианта воплощения изобретения могут быть объединены с любым одним или более другими признаками любого другого варианта воплощения изобретения без отступления от объема изобретения.

Кроме того, следует понимать, что описанное выше настоящее изобретение может быть реализовано в виде логической схемы управления с использованием программного обеспечения модульным или интегрированным способом. На основе представленных в данном документе описания и идей специалист в данной области техники узнает и поймет другие способы реализации настоящего изобретения с использованием аппаратного обеспечения и комбинации аппаратного обеспечения и программного обеспечения.

Элементы, указанные в единственном числе, подразумевают значение "один или более", если специально не указано иначе.

Формула изобретения

1. Устройство для аутентификации потребителя, проводящего платежную транзакцию с использованием мобильного устройства, причем устройство содержит:

процессор, запрограммированный для исполнения набора инструкций;

носитель данных, присоединенный к процессору; и

причем набор инструкций содержится на носителе данных, при этом, когда набор инструкций исполняется процессором, устройство аутентифицирует потребителя посредством:

регистрации мобильного устройства и связи мобильного устройства с платежным счетом потребителя;

аутентификации регистрации мобильного устройства с использованием идентификационных данных, ранее предоставленных потребителем и связанных с платежным счетом;

приема данных, инициирующих платежную транзакцию;

определения, что платежная транзакция была инициирована с использованием мобильного устройства; и

определения, основываясь на аутентификации регистрации мобильного устройства, что платежная транзакция аутентифицирована для платежного счета с использованием мобильного устройства.

2. Устройство по п.1, в котором регистрация мобильного устройства и связь мобильного устройства с платежным счетом потребителя дополнительно содержит:

прием регистрационных данных от потребителя, причем

регистрационные данные включают в себя идентификатор платежного счета и идентификатор мобильного устройства, при этом регистрационные данные обеспечиваются потребителем с использованием клиентского устройства.

3. Устройство по п. 2, в котором мобильное устройство представляет собой мобильный телефон и идентификатор мобильного устройства представляет собой

номер телефона мобильного телефона.

4. Устройство по п. 2, в котором регистрационные данные обеспечиваются потребителем посредством ввода регистрационных данных на веб-сайт с использованием клиентского устройства.

5. Устройство по п.1, в котором аутентификация регистрации мобильного устройства с использованием идентификационных данных, ранее предоставленных потребителем и связанных с платежным счетом, дополнительно содержит:

запрос потребителя обеспечить идентификационные данные;

прием запрошенных идентификационных данных;

определение, что принятые идентификационные данные согласуются с идентификационными данными, ранее предоставленными потребителем и связанными с платежным счетом; и

в ответ на определение, что принятые идентификационные данные согласуются с идентификационными данными, ранее предоставленными потребителем, определение, что регистрация мобильного устройства аутентифицирована.

6. Устройство по п.5, в котором идентификационные данные представляют собой пароль, ранее связанный с платежным счетом и используемый потребителем для одобрения платежной транзакции.

7. Устройство по п.1, в котором после определения, что платежная транзакция была инициирована с использованием мобильного устройства, устройство аутентифицирует потребителя посредством контакта с потребителем через мобильное устройство для получения подтверждения, что потребитель желает завершить платежную транзакцию.

8. Устройство по п.7, в котором контакт с потребителем через мобильное устройство дополнительно содержит контакт с потребителем посредством одного или более из формирования вызова на мобильное устройство или формирования сообщения на мобильное устройство.

9. Устройство по п.1, в котором после определения, что платежная транзакция была инициирована с использованием мобильного устройства, устройство аутентифицирует потребителя посредством:

запроса потребителя обеспечить второй вид идентификационных данных, причем второй вид идентификационных данных ранее зарегистрирован для использования при аутентификации платежных транзакций, инициируемых с использованием мобильного устройства;

приема второго вида идентификационных данных от мобильного устройства; и

верификации, что принятый второй вид идентификационных данных корректен.

10. Устройство по п.1, в котором платежная транзакция обрабатывается после определения, что платежная транзакция аутентифицирована для платежного счета с использованием мобильного устройства.

11. Способ аутентификации потребителя, проводящего платежную транзакцию с использованием мобильного устройства, причем способ содержит:

прием данных, идентифицирующих мобильное устройство, и данных, идентифицирующих платежный счет потребителя;

аутентификацию мобильного устройства с использованием идентификационных данных, ранее предоставленных потребителем и связанных с платежным счетом;

прием данных, инициирующих платежную транзакцию;

определение, что платежная транзакция была инициирована с использованием мобильного устройства; и

определение, основываясь на аутентификации мобильного устройства, что платежная

транзакция аутентифицирована для платежного счета с использованием мобильного устройства.

12. Способ по п.11, в котором платежная транзакция обрабатывается после определения, что платежная транзакция аутентифицирована для платежного счета с использованием мобильного устройства.

13. Способ по п.11, в котором мобильное устройство представляет собой мобильный телефон, и данные, идентифицирующие мобильное устройство, представляют собой номер телефона для мобильного телефона.

14. Способ по п.11, в котором аутентификация мобильного устройства с использованием идентификационных данных, ранее предоставленных потребителем и связанных с платежным счетом, дополнительно содержит:

запрос потребителя обеспечить идентификационные данные;

прием запрошенных идентификационных данных;

определение, что принятые идентификационные данные согласуются с идентификационными данными, ранее предоставленными потребителем и связанными с платежным счетом; и

в ответ на определение, что принятые идентификационные данные согласуются с идентификационными данными, ранее предоставленными потребителем, определение, что мобильное устройство аутентифицировано.

15. Способ по п.11, в котором после определения, что платежная транзакция была инициирована с использованием мобильного устройства, способ дополнительно содержит осуществление контакта с потребителем через мобильное устройство для получения подтверждения, что потребитель желает завершить платежную транзакцию.

16. Способ по п.15, в котором контакт с потребителем через мобильное устройство дополнительно содержит осуществление контакта с потребителем посредством одного или более из формирования вызова на мобильное устройство или формирования сообщения на мобильное устройство.

17. Способ по п.11, в котором после определения, что платежная транзакция была инициирована с использованием мобильного устройства, способ дополнительно содержит:

запрос потребителя обеспечить второй вид идентификационных данных, причем второй вид идентификационных данных ранее зарегистрирован для использования при аутентификации платежных транзакций, инициированных с использованием мобильного устройства;

прием второго вида идентификационных данных от мобильного устройства; и

верификацию, что принятый второй вид идентификационных данных корректен.

18. Способ проведения платежной транзакции, причем способ содержит:

связывание платежного счета потребителя с первыми идентификационными данными потребителя, при этом первые идентификационные данные потребителя используются потребителем для одобрения платежных транзакций, осуществляемых с использованием платежного счета потребителя;

прием данных, идентифицирующих мобильное устройство, и данных, идентифицирующих платежный счет потребителя;

запрос потребителя обеспечить первые идентификационные данные потребителя;

аутентификацию мобильного устройства, если ответ на запрос представляет собой первые идентификационные данные потребителя;

прием данных, инициирующих платежную транзакцию; и

определение, что платежная транзакция была инициирована с использованием

мобильного устройства; и

в ответ на определение, что платежная транзакция была инициирована с использованием мобильного устройства, определение, основываясь на аутентификации мобильного устройства, что платежная транзакция аутентифицирована для платежного счета потребителя с использованием мобильного устройства.

19. Способ по п.18, дополнительно содержащий: обработку платежной транзакции без требования, чтобы потребитель участвовал в процессе аутентификации во время платежной транзакции.

20. Способ по п.18, в котором мобильное устройство представляет собой мобильный телефон, и данные, идентифицирующие мобильное устройство, представляют собой номер телефона для мобильного телефона.

21. Способ по п.18, в котором запрос потребителя обеспечить первые идентификационные данные потребителя дополнительно содержит прием от потребителя вторых идентификационных данных потребителя, при этом вторые идентификационные данные потребителя установлены для использования потребителем для одобрения платежных транзакций, осуществляемых с использованием мобильного устройства, и аутентификация потребителя дополнительно содержит прием от потребителя вторых идентификационных данных потребителя для того, чтобы авторизовать платежную транзакцию.

22. Способ привязки мобильного устройства к платежному счету, причем способ содержит:

a) прием, на компьютере мобильной платежной системы (MPI) продавца, данных, идентифицирующих мобильное устройство, и данных, идентифицирующих платежный счет потребителя;

b) определение сервера управления доступом к эмитенту, связанного с платежным счетом;

c) передачу компьютером MPI продавца запроса аутентификации, включающего в себя данные, идентифицирующие мобильное устройство, и данные, идентифицирующие платежный счет, серверу

управления доступом к эмитенту, при этом сервер управления доступом к эмитенту впоследствии:

передает веб-страницу на клиентское устройство, управляемое потребителем;

принимает данные аутентификации от клиентского устройства через переданную веб-страницу;

верифицирует принятые данные аутентификации, основываясь на данных аутентификации, ранее предоставленных для платежного счета потребителем серверу управления доступом к эмитенту; и

формирует результат аутентификации, основываясь на верификации принятых данных аутентификации;

d) прием компьютером MPI продавца результата аутентификации; и

e) пересылку компьютером MPI продавца результата аутентификации на компьютер эмитента, управляемый эмитентом, при этом эмитент впоследствии определяет, что платежный счет активен;

посредством этого осуществляется регистрация мобильного устройства с платежным счетом.

23. Способ по п.22, в котором определение сервера управления доступом к эмитенту, связанного с платежным счетом, содержит идентификацию, основываясь на данных, идентифицирующих платежный счет, сервера управления доступом к эмитенту из

множества серверов управления доступом к эмитенту с использованием сервера каталогов.

24. Способ по п.22, в котором передача запроса аутентификации, включающего в себя данные, идентифицирующие мобильное устройство, и данные, идентифицирующие платежный счет, происходит через сервер каталогов.

25. Способ по п.22, в котором данные, идентифицирующие мобильное устройство, представляют собой номер телефона и данные, идентифицирующие платежный счет, представляют собой номер платежного счета.

26. Способ по п.22, в котором данные аутентификации содержат пароль.

27. Способ по п.22, в котором клиентское устройство представляет собой мобильное устройство.

28. Способ по п.22, в котором сервер управления доступом к эмитенту, клиентское устройство и компьютер MPI продавца отделены друг от друга.

29. Способ по п.22, в котором сервер управления доступом к эмитенту цифровым образом подписывает результат аутентификации.

30. Способ по п.22, в котором передача запроса аутентификации, включающего в себя данные, идентифицирующие мобильное устройство, и данные, идентифицирующие платежный счет, происходит через сервер каталогов, и при этом сервер каталогов находится в сети обработки платежей.

31. Способ по п.22, в котором передача запроса аутентификации, включающего в себя данные, идентифицирующие мобильное устройство, и данные, идентифицирующие платежный счет, происходит через сервер каталогов, и при этом сервер каталогов находится в сети обработки платежей, которая сконфигурирована для обработки кредитовых и дебетовых транзакций по картам и которая сконфигурирована для выполнения авторизации и расчетно-клиринговых служб.

32. Компьютер мобильной платежной системы (MPI) продавца, содержащий процессор и считываемый компьютером носитель, присоединенный к процессору, причем считываемый компьютером носитель содержит код, исполняемый процессором для реализации способа содержащего:

a) прием, на компьютере MPI продавца, данных, идентифицирующих мобильное устройство, и данных, идентифицирующих платежный счет потребителя;

b) определение сервера управления доступом к эмитенту, связанного с платежным счетом;

c) передачу компьютером MPI продавца запроса авторизации, включающего в себя данные, идентифицирующие мобильное устройство, и данные, идентифицирующие платежный счет, серверу управления доступом к эмитенту, при этом сервер управления доступом к эмитенту впоследствии:

передает веб-страницу на клиентское устройство, управляемое потребителем;

принимает данные аутентификации от клиентского устройства через переданную веб-страницу;

верифицирует принятые данные аутентификации, основываясь на данных аутентификации, ранее предоставленных для платежного счета потребителем серверу управления доступом к эмитенту; и

формирует результат аутентификации, основываясь на верификации принятых данных аутентификации;

d) прием компьютером MPI продавца результата аутентификации; и

e) пересылку компьютером MPI продавца результата аутентификации на компьютер

эмитента, управляемый эмитентом, при этом эмитент впоследствии определяет, что платежный счет активен;

посредством этого осуществляется регистрация мобильного устройства с платежным счетом.

33. Компьютер MPI продавца по п.32, в котором определение сервера управления доступом к эмитенту, связанного с платежным счетом, содержит идентификацию, основываясь на данных, идентифицирующих платежный счет, сервера управления доступом к эмитенту из множества серверов управления доступом к эмитенту с использованием сервера каталогов.

34. Компьютер MPI продавца по п.32, в котором передача запроса аутентификации, включающего в себя данные, идентифицирующие мобильное устройство, и данные, идентифицирующие платежный счет, происходит через сервер каталогов.

35. Компьютер MPI продавца по п.32, в котором данные, идентифицирующие мобильное устройство, представляют собой номер телефона и данные, идентифицирующие платежный счет, представляют собой номер платежного счета.

36. Компьютер MPI продавца по п.32, в котором данные аутентификации содержат пароль.

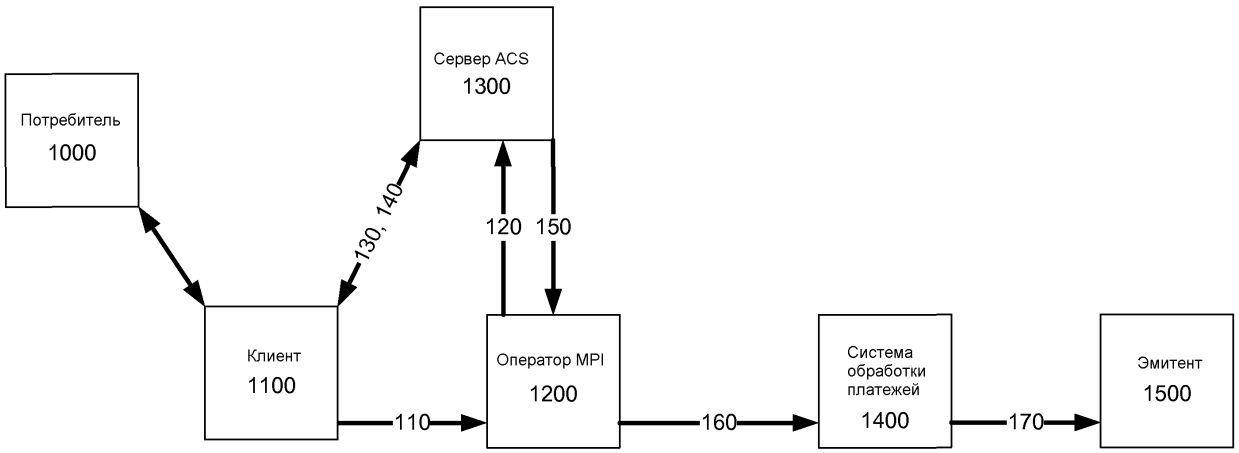
37. Компьютер MPI продавца по п.32, в котором клиентское устройство представляет собой мобильное устройство.

38. Компьютер MPI продавца по п.32, в котором сервер управления доступом к эмитенту, клиентское устройство и компьютер MPI продавца отделены друг от друга.

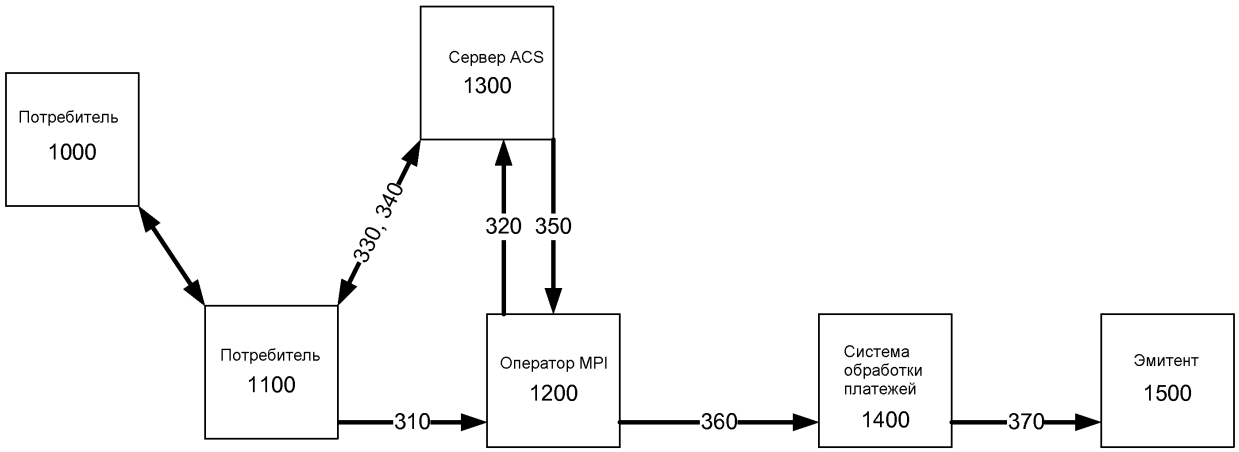
39. Компьютер MPI продавца по п.32, в котором сервер управления доступом к эмитенту цифровым образом подписывает результат аутентификации.

40. Компьютер MPI продавца по п.32, в котором передача запроса аутентификации, включающего в себя данные, идентифицирующие мобильное устройство, и данные, идентифицирующие платежный счет, происходит через сервер каталогов, и при этом сервер каталогов находится в сети обработки платежей.

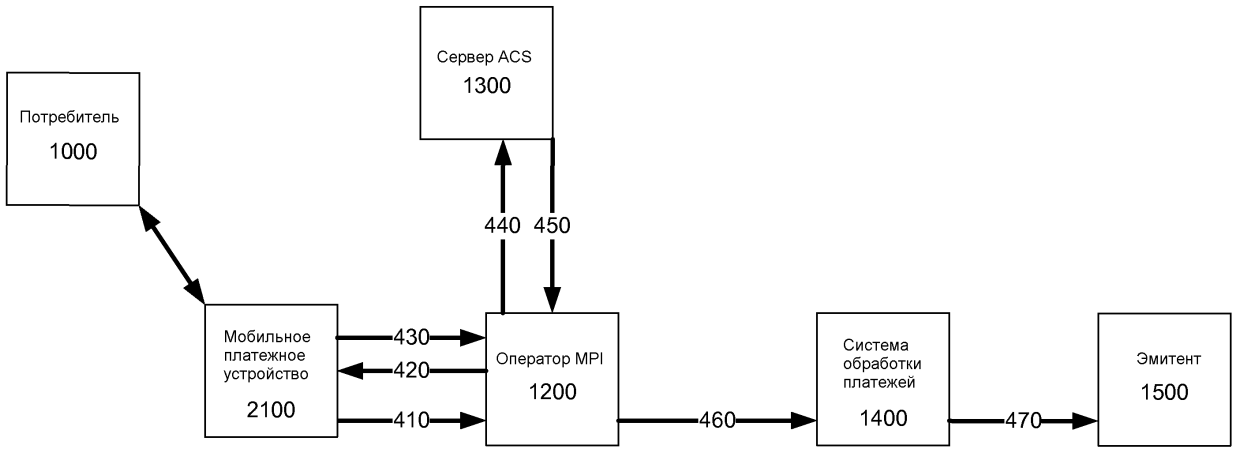
41. Компьютер MPI продавца по п.32, в котором передача запроса аутентификации, включающего в себя данные, идентифицирующие мобильное устройство, и данные, идентифицирующие платежный счет, происходит через сервер каталогов, и при этом сервер каталогов находится в сети обработки платежей, которая сконфигурирована для обработки кредитовых и дебетовых транзакций по картам и которая сконфигурирована для выполнения авторизации и расчетно-клиринговых служб.



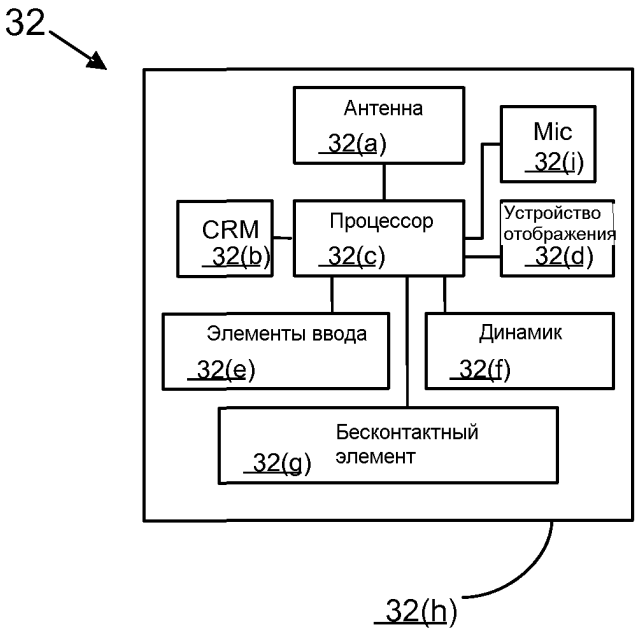
Фиг. 1



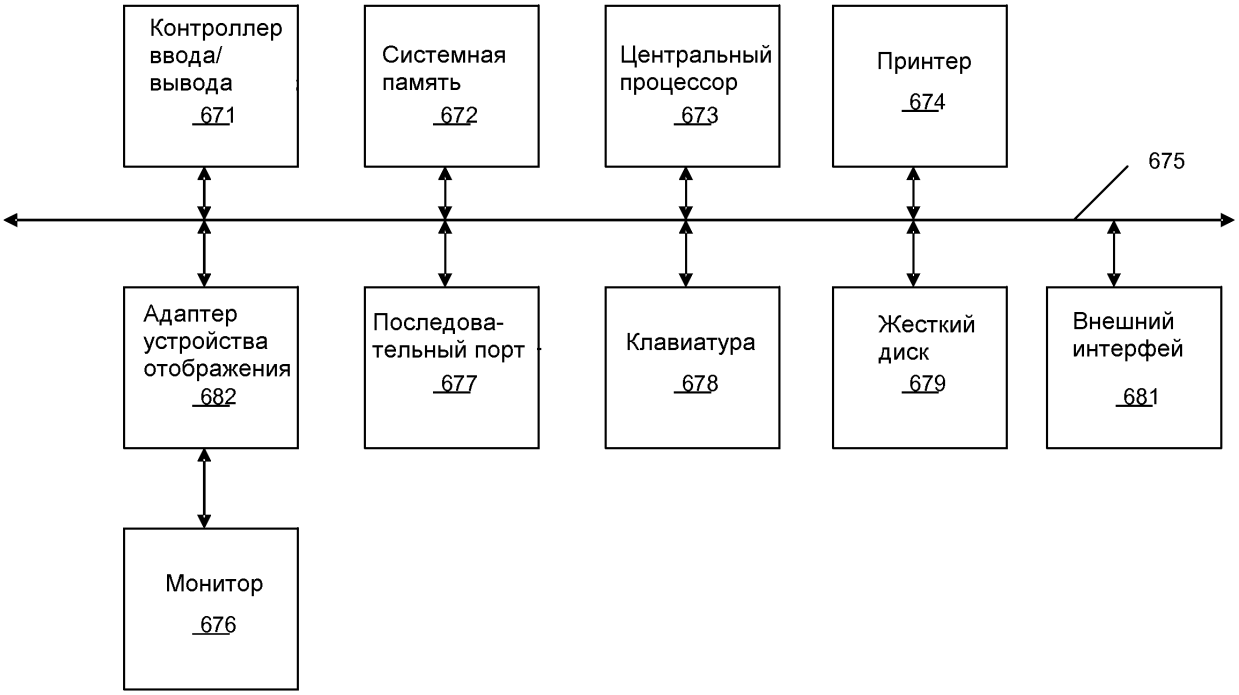
Фиг. 3



Фиг. 4


32
Антенна
32(a)
Mic
32(j)
CRM
32(b)
Процессор
32(c)
Устройство отображения
32(d)
Элементы ввода
32(e)
Динамик
32(f)
Бесконтактный элемент
32(g)
32(h)

Фиг. 5


Контроллер ввода/ вывода
671
Системная память
672
Центральный процессор
673
Принтер
674
675
Адаптер устройства отображения
682
Последова-тельный порт
677
Клавиатура
678
Жесткий диск
679
Внешний интерфей
681
Монитор
676

Фиг. 6