



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК

G06Q 20/045 (2006.01); G06Q 20/20 (2006.01); G06Q 20/32 (2006.01); G06Q 20/3274 (2006.01); G06Q 30/02 (2006.01)

(21)(22) Заявка: 2014129856, 19.12.2012

(24) Дата начала отсчета срока действия патента:
19.12.2012

Дата регистрации:
02.03.2018

Приоритет(ы):

(30) Конвенционный приоритет:
19.12.2011 US 61/577,652;
16.04.2012 US 13/448,193

(43) Дата публикации заявки: 10.02.2016 Бюл. № 4

(45) Опубликовано: 02.03.2018 Бюл. № 7

(85) Дата начала рассмотрения заявки РСТ на
национальной фазе: 21.07.2014

(86) Заявка РСТ:
US 2012/070683 (19.12.2012)

(87) Публикация заявки РСТ:
WO 2013/096486 (27.06.2013)

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

(72) Автор(ы):

БРАДНИКИ Дэвид (US),
КРАФТ Майкл (US),
РЕЙСГИС Ханс (US),
ВАЙНШТЕЙН Эндрю (US)

(73) Патентообладатель(и):

СИКВЕНТ СОФТВЭР ИНК. (US)

(56) Список документов, цитированных в отчете
о поиске: US 2008/0116264 A1, 22.05.2008. RU
2273049 C2, 27.03.2006. RU 2402814 C2,
27.10.2010. US 2011/0153495 A1, 23.06.2011. US
2011/153498 A1, 23.06.2011.

(54) СИСТЕМА И СПОСОБ ДИНАМИЧЕСКОГО ВРЕМЕННОГО РАЗРЕШЕНИЯ НА ПЛАТЕЖ В ПЕРЕНОСНОМ УСТРОЙСТВЕ СВЯЗИ

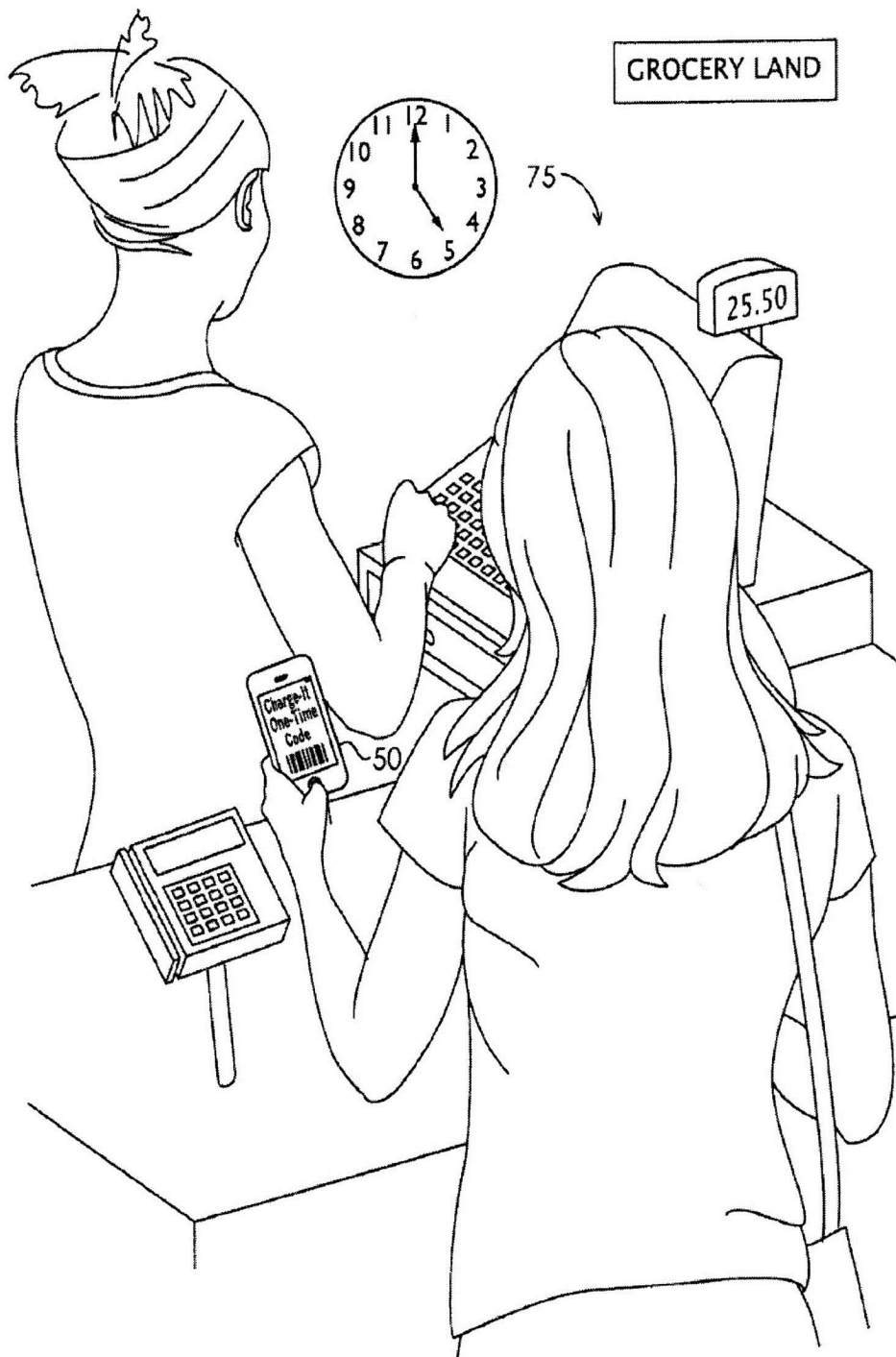
(57) Реферат:

Изобретение относится к проверке проведения транзакции с динамическими временными идентификационными данными для переносного устройства связи, применяемого в транзакции с точкой электронного управления, например торговой точкой, точкой доступа к беспроводной связи ближнего радиуса действия. Технический результат заключается в расширении арсенала средств для проверки проведения транзакций.

Переносное устройство связи содержит модуль, определяющий географическое местоположение, например модуль глобальной системы позиционирования. Система содержит централизованный модуль, получающий данные о текущем географическом местоположении переносного устройства связи, передающий динамические временные идентификационные данные на переносное устройство связи и

предоставляющий прогнозную информацию о транзакции, включая динамические временные идентификационные данные и данные о географическом местоположении переносного устройства связи, в систему авторизации, функционально связанную с точкой электронного управления. Динамические временные идентификационные данные обладают заранее определенным временем жизни, что обеспечивает

возможность рециркуляции динамических идентификационных данных, причем такая рециркуляция может принимать во внимание географическое местоположение, для которого были недавно выпущены идентификационные данные. Также описан способ использования динамических временных идентификационных данных с переносным устройством связи. 2 н. и 13 з.п. ф-лы, 10 ил., 1 табл.



Фиг. 1А



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) **ABSTRACT OF INVENTION**

(52) CPC

G06Q 20/045 (2006.01); *G06Q 20/20* (2006.01); *G06Q 20/32* (2006.01); *G06Q 20/3274* (2006.01); *G06Q 30/02* (2006.01)

(21)(22) Application: **2014129856, 19.12.2012**(24) Effective date for property rights:
19.12.2012Registration date:
02.03.2018

Priority:

(30) Convention priority:
19.12.2011 US 61/577,652;
16.04.2012 US 13/448,193(43) Application published: **10.02.2016** Bull. № 4(45) Date of publication: **02.03.2018** Bull. № 7(85) Commencement of national phase: **21.07.2014**(86) PCT application:
US 2012/070683 (19.12.2012)(87) PCT publication:
WO 2013/096486 (27.06.2013)Mail address:
129090, Moskva, ul. B. Spasskaya, 25, stroenie 3,
OOO "Yuridicheskaya firma Gorodisskij i Partnery"

(72) Inventor(s):

BRADNIKI Devid (US),
KRAFT Majkl (US),
REJSGIS Khans (US),
VAJNSHTEJN Endryu (US)

(73) Proprietor(s):

SIKVENT SOFTVER INK. (US)(54) **SYSTEM AND METHOD OF DYNAMIC TIME PERMIT ON PAYMENT IN PORTABLE COMMUNICATION DEVICE**

(57) Abstract:

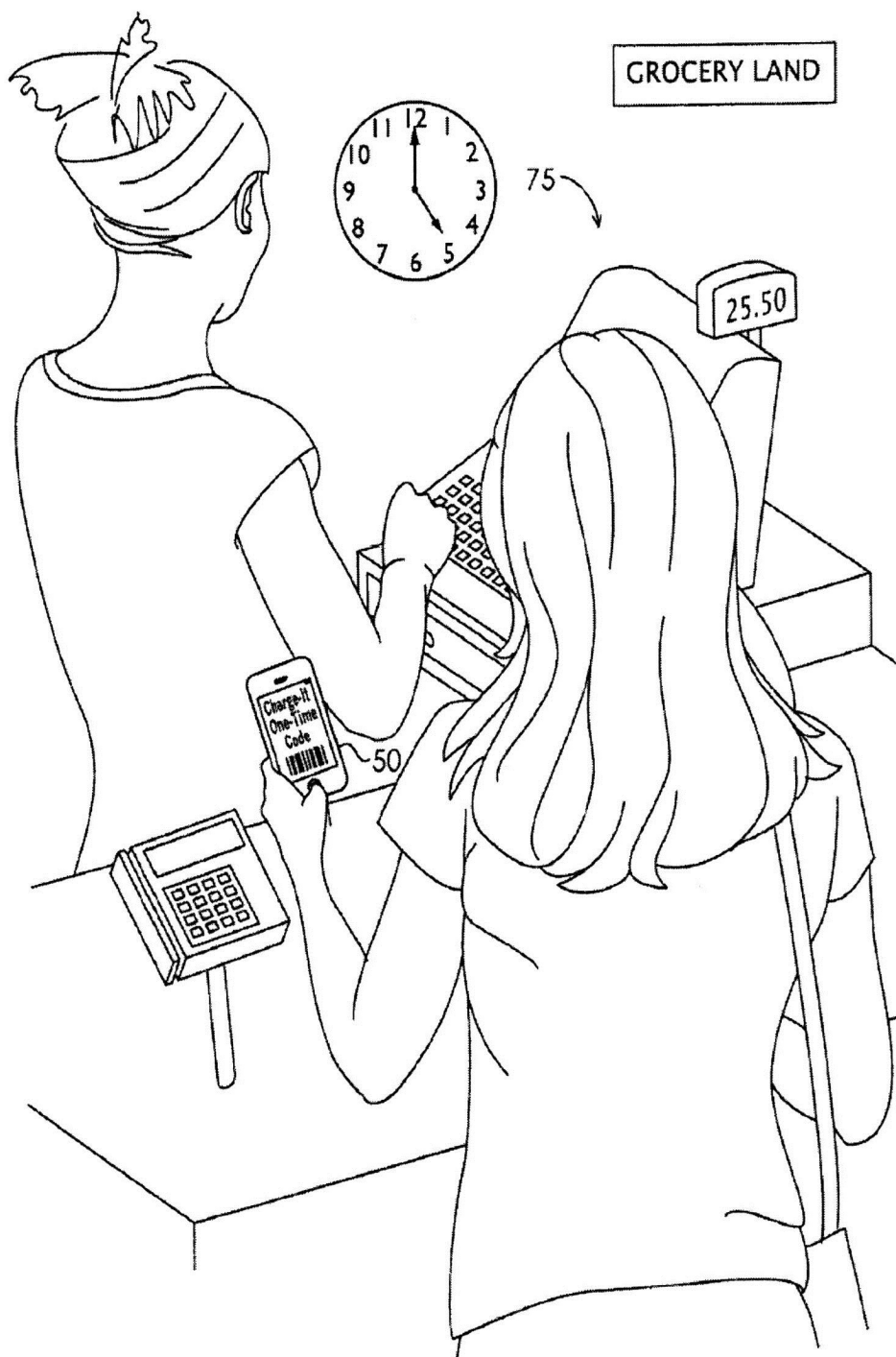
FIELD: information technology.

SUBSTANCE: invention relates to verifying transaction with dynamic time identification data for a portable communication device used in transaction with an electronic control point, for example, a sales point, a short-range wireless access point. Portable communication device contains a module that determines a geographic location, for example, a global positioning system module. System comprises a centralized module receiving data on the current geographic location of the portable communication

device transmitting the dynamic temporary identification data to the portable communication device and providing prediction information about the transaction, including dynamic temporary identification data and geographic location data of the portable communication device, to an authorization system operatively associated with the electronic control point. Dynamic time identification data has a predetermined lifetime, which enables the recycling of dynamic identification data, such recycling being able to take into account the geographic location for which the

identification data was recently released. Method for using dynamic temporary identification data with a portable communication device is also described.

EFFECT: technical result consists in expanding the arsenal of means to verify the conduct of transactions.
15 cl, 10 dwg, 1 tbl



Фиг. 1А

RU 2646331 C2

RU 2646331 C2

[0001] Настоящая заявка испрашивает приоритет согласно предварительной заявке на патент США №61/577652, поданной 19 декабря 2011 г., и обычной заявке на патент США №13/448193, поданной 16 апреля 2012 г., причем содержание обоих заявок полностью включено в настоящую заявку посредством ссылки.

5 Область техники

[0002] Изобретение в целом относится к использованию безопасных данных для выполнения беспроводной транзакции и, в частности, к системе и способу для обработки транзакции разового платежа по запросу от переносного устройства связи, что может быть основано на информации о географическом местоположении в физическом мире.

10 Уровень техники

[0003] Беспроводные транзакции, использующие основанные на радиочастотной идентификации карточки бесконтактного считывания, весьма распространены. Например, многие рабочие используют магнитные карточки с радиочастотной идентификацией для получения доступа к своим рабочим местам, а водители используют пропуск с радиочастотной идентификацией для оплаты сборов на магистралях. При радиочастотной идентификации электромагнитные волны используют для обмена данными между терминалом и некоторым объектом с целью идентификации. В последнее время некоторые компании пытались использовать радиочастотную идентификацию, поддерживаемую мобильными телефонами, для реализации электронного платежного инструмента (например, кредитной и/или дебетовой карточки). Однако базовая технология радиочастотной идентификации поднимает много связанных с безопасностью проблем, что требует модификации базовой технологии. Однако широко распространенное принятие радиочастотной идентификации в качестве механизма для электронных платежей было медленным.

25 [0004] Также быстро растет использование смартфонов пользователями. Возникла задача предоставления пользователям возможности выполнения электронных платежей посредством использования имеющихся у них мобильных телефонов. Технология беспроводной связи ближнего радиуса действия (NFC) в телефонах со встроенными элементами безопасности обеспечивает возможность одного потенциального решения этой задачи.

[0005] Беспроводная связь ближнего радиуса действия представляет собой еще одну технологию, которая, как и радиочастотная идентификация, использует электромагнитные волны для обмена данными. Беспроводная связь ближнего радиуса действия представляет собой открытый стандарт (см., например, стандарт ISO/IEC 35 18092), определяющий схемы модуляции, кодирование, скорости передачи и радиочастотный интерфейс. В отличие от радиочастотной идентификации волны в технологии беспроводной связи ближнего радиуса действия передают только по короткому пути (порядка нескольких дюймов) и на высоких частотах. Таким образом, имело место более широкое принятие беспроводной связи ближнего радиуса действия в качестве коммуникационной платформы, поскольку она обеспечивает лучшую безопасность для финансовых операций и управления доступом. Известны другие протоколы ближней связи, приемлемые для использования при поддержке финансовых транзакций и управления доступом.

45 [0006] Устройства беспроводной связи ближнего радиуса действия уже находят применение для выполнения платежей в кассовых терминалах. Но существует много кассовых терминалов, не обеспечивающих возможность беспроводной связи ближнего радиуса действия. В соответствии с этим настоящее изобретение имеет целью техническое решение, обеспечивающему любому смартфону возможность проведения в высшей

степени безопасных электронных платежей в торговых точках, принимающих обычные электронные платежи посредством обычного кассового терминала.

[0007] Другая проблема состоит в очень большом количестве коммуникационных протоколов, связанных со всевозможными существующими кассовыми терминалами. Так, например, протокол, необходимый для успешной связи посредством беспроводных технологий с кассовым терминалом производства компании IBM, может быть сильно отличен от протокола, необходимого для связи с кассовым терминалом производства компании NCR. В соответствии с этим цель настоящего изобретения состоит в создании системы и способа, предназначенных для использования данных о географическом местоположении (при их наличии), чтобы попытаться заранее определить кассовый терминал в вероятной торговой точке, присутствующий в предприятии розничной торговли, размещенном там же, где и переносное устройство связи.

[0008] Возможность принятия физическими торговыми точками платежей в электронной форме существенно выросла в развитых странах и быстро растет в развивающихся странах. Финансовая отрасль разработала и ввела в действие строгие системы, способы и требования к электронным транзакциям с целью подавления и сведения к минимуму мошеннического поведения.

[0009] В соответствии с этим настоящее изобретение также имеет целью обеспечение одного технического решения или большего количества технических решений относительно предшествующих возможностей и связанных с ними проблем, как это может быть понято специалистами в данной области техники при рассмотрении ими настоящего описания. Эти и другие цели и преимущества настоящего изобретения также будут очевидны для специалистов в данной области техники при рассмотрении ими настоящих чертежей, спецификаций и пунктов формулы изобретения. Совершенно понятно, что все такие дополнительные системы, способы, функции и отличительные признаки содержатся в рамках этого описания, не выходят за пределы объема настоящего изобретения и защищены прилагаемыми пунктами формулы изобретения.

Краткое описание чертежей

[0010] Для лучшего понимания сути настоящего изобретения неограничивающие и неисчерпывающие варианты реализации описаны со ссылками на последующие чертежи. На этих чертежах, если не указано иное, одинаковые номера позиций относятся к одинаковым частям на всех различных чертежах.

[0011] На фиг. 1А показан конечный пользователь, пытающийся использовать свое переносное устройство связи для проведения защищенной транзакции платежа в торговой точке.

[0012] На фиг. 1В показаны действующие соединения между смартфоном конечного пользователя (то есть переносным устройством связи) и различными подсистемами, включая оконечный интерфейс управления системой.

[0013] На фиг. 2 показана блок-схема, иллюстрирующая некоторые из логических блоков в пределах переносного устройства связи, которые могут иметь отношение к настоящей системе.

[0014] Фиг. 3А и 3В вместе иллюстрируют один потенциальный вариант реализации настоящего изобретения относительно последовательности операций при разовом платеже.

[0015] На фиг. 4 показана блок-схема, иллюстрирующая информационный поток между переносным устройством связи и остальной частью платежной экосистемы в связи с последовательностью операций при разовом платеже по фиг. 3А и 3В.

[0016] Фиг. 5, 6 и 6А представляют собой иллюстрации взятого в качестве примера

и представляющего собой кошелек интерфейса пользователя, который может быть развернут на смартфоне.

[0017] Фиг. 7А и 7В представляют собой иллюстрации двух потенциальных вариантов реализации идентификационных данных для выполнения разового платежа, выработанных взятым в качестве примера и представляющим собой кошелек интерфейсом пользователя на обычном переносном устройстве связи.

[0018] На фиг. 8А показана блок-схема, иллюстрирующая некоторые из логических блоков в пределах переносного устройства связи, которые могут иметь отношение к настоящей системе.

[0019] На фиг. 8В показана блок-схема, иллюстрирующая дополнительные подробности блока «кошелек для выполнения разового платежа» по фиг. 8А, который может иметь отношение к настоящей системе.

[0020] Фиг. 9А и 9В вместе иллюстрируют один потенциальный вариант реализации интерфейса пользователя, который может быть реализован на взятом в качестве примера смартфоне, дополнительно показывающий гибкость функциональных возможностей разовых идентификационных данных вместе с объединенным кошельком.

[0021] На фиг. 10 показана блок-схема одного потенциального варианта реализации системы, лежащей в основе предоставления разрешения приложению разового платежа на просмотр, выбор и/или изменение безопасных данных, хранимых в платежной подсистеме.

Подробное описание изобретения

[0022] Настоящее изобретение теперь будет описано более подробно со ссылками на прилагаемые чертежи, которые образуют его часть и которые показывают, посредством иллюстрации, определенные варианты реализации, посредством которых изобретение может быть выполнено. Однако настоящее изобретение может быть выполнено во многих различных формах и не должно быть рассмотрено, как ограниченное сформулированными здесь вариантами реализации изобретения; скорее эти варианты реализации изобретения приведены таким образом, чтобы это раскрытие было аккуратным и полным и полностью сообщало объем изобретения специалистам в данной области техники. Между прочим, отметим, что настоящее изобретение может быть выполнено в виде способов или устройств. В соответствии с этим настоящее изобретение и его компоненты могут принимать форму полностью аппаратного варианта реализации, полностью программного варианта реализации или варианта реализации, комбинирующего особенности программного и аппаратного обеспечения. Последующее подробное описание изобретения, следовательно, не должно быть рассмотрено в ограничивающем смысле.

Переносные устройства связи

[0023] Настоящее изобретение предлагает систему и способ, которые могут быть использованы со множеством различных переносных устройств связи, включая, но не ограничиваясь этим, персональные цифровые секретари, сотовые телефоны, смартфоны, ноутбуки, планшетные компьютеры и другие мобильные устройства, которые предпочтительно содержат сотовую службу речи и данных, а также, предпочтительно, обеспечивают доступ к приложениям, способным быть загруженными пользователем. Одно такое переносное устройство связи может быть типа iPhone, Motorola RAZR или DROID; однако предпочтительно, чтобы настоящее изобретение не зависело от платформ и устройств. Например, технологическая платформа переносного устройства связи может быть платформой типа Microsoft Windows Mobile, Microsoft Windows Phone 7, Palm OS, RIM Blackberry OS, Apple OS, Android OS, Symbian, Java или любой другой

технологической платформой. Для целей этого раскрытия настоящее изобретение в целом описано в соответствии с функциями и интерфейсами, оптимизированными для смартфона, использующего обобщенную платформу, хотя специалисту в данной области техники понятно, что все такие функции и интерфейсы могут также быть использованы и адаптированы для любых других платформ и/или устройств.

[0024] Переносное устройство связи содержит одно устройство электромагнитной связи с коротким радиусом действия или большее количество таких устройств, таких как устройства беспроводной связи ближнего радиуса действия, устройства радиочастотной идентификации или приемопередатчик типа Bluetooth. В настоящее время предпочтительно использовать основную полосу беспроводной связи ближнего радиуса действия, которая совместима со стандартами NFC IP 1 (www.nfcforum.org), обеспечивающими стандартные функции, такие как обмен одноранговыми данными, режим «устройство считывания - устройство записи» (то есть сбор информации от тегов радиочастотной идентификации) и эмуляция бесконтактной карточки (в соответствии со стандартами NFC IP 1 и ISO 14443), при соединении с элементом безопасности на переносном устройстве связи и представлении перед «бесконтактным устройством считывания платежа» (см. ниже в торговой точке). Как очевидно для специалистов в данной области техники, имеющих настоящее описание, чертежи и пункты формулы изобретения, стандарты NFC IP 1 представляют собой просто предпочтительный в настоящее время пример, который может быть экспортирован (полностью или частично) для использования совместно с любым другим стандартом связи ближнего радиуса действия. Кроме того, предпочтительно, чтобы переносное устройство связи содержало антенну (беспроводной связи ближнего радиуса действия / радиочастотной идентификации) (согласно стандартам NFC IP 1 и ISO 14443) для выполнения беспроводной связи ближнего радиуса действия. Однако как очевидно специалистам в данной области техники (беспроводная связь ближнего радиуса действия / радиочастотная идентификация), могут быть выполнены даже при наличии более коротких диапазонов и потенциальных проблем со считыванием.

[0025] Переносное устройство связи также содержит мобильный сетевой интерфейс, предназначенный для установления беспроводной связи с мобильным сетевым оператором и управления ею. Мобильный сетевой интерфейс использует один протокол и одну технологию связи или большее количество протоколов и технологий связи, включая, но не ограничиваясь этим, глобальную систему для мобильной связи (GSM), третье поколение мобильных сетей (3G), четвертое поколение мобильных сетей (4G), множественный доступ с кодовым разделением каналов (CDMA), множественный доступ с временным разделением каналов (TDMA), протокол пользовательских дейтаграмм (UDP), протокол управления передачей / Протокол Интернета (TCP/IP), службу коротких сообщений (SMS), общую службу пакетной радиосвязи (GPRS), протокол беспроводного доступа (WAP), сверхширокую полосу пропускания (UWB), протокол IEEE 802.16 глобальной совместимости для микроволнового доступа (WiMax), протокол SIP/RTP или любой протокол из множества других протоколов беспроводной связи, предназначенных для связи с мобильной сетью оператора мобильной связи. В соответствии с этим мобильный сетевой интерфейс может содержать в качестве приемопередатчика приемно-передающее устройство или сетевую интерфейсную плату. Совершенно понятно, что мобильный сетевой интерфейс и электромагнитное устройство связи с коротким радиусом действия могут совместно использовать приемопередатчик или приемно-передающее устройство, как очевидно для специалистов в данной области техники, имеющих настоящее описание, чертежи и пункты формулы изобретения.

[0026] Переносное устройство связи кроме того содержит приемопередатчик местоположения, способный определять физические координаты устройства на поверхности Земли, обычно в виде функции ее широты, долготы и высоты. Такой приемопередатчик местоположения предпочтительно использует технологию

5 глобальной системы позиционирования (GPS), так что он может быть назван здесь приемопередатчиком глобальной системы позиционирования; однако совершенно понятно, что приемопередатчик местоположения способен дополнительно (или в качестве альтернативы) использовать другие приспособления для определения географического местоположения, включая, но не ограничиваясь этим, триангуляцию,

10 принудительную глобальную систему позиционирования (AGPS), оптоэлектронное устройство сопровождения (E-OTD), системы CI, SAI, ETA, BSS и т.п., предназначенные для определения физического местоположения переносного устройства связи на поверхности Земли.

[0027] Переносное устройство связи, кроме того, содержит интерфейс пользователя,

15 предоставляющий пользователю средства для получения информации, а также для введения информации или для ответа иным образом на полученную информацию. Как теперь понятно (без намерения ограничить настоящее раскрытие изобретения), этот интерфейс пользователя может содержать микрофон, динамик, тактильный интерфейс, графический дисплей, клавишную панель, клавиатуру, манипулятор и/или сенсорный

20 экран. Переносное устройство связи будет также содержать микропроцессор и память большого объема. Память большого объема может содержать постоянное запоминающее устройство (ROM), запоминающее устройство с произвольной выборкой (RAM), а также одну съемную карту памяти или большее количество таких карт. Память большого объема обеспечивает хранение машинно-читаемых команд и других данных,

25 включая базовую систему ввода-вывода (BIOS) и операционную систему, предназначенную для управления работой переносного устройства связи.

[0028] Переносное устройство связи будет также содержать память идентификации устройства, предназначенную для идентификации устройства, например, карточку модуля идентификации абонента (SIM). В обычном понимании карточка модуля

30 идентификации абонента содержит уникальный электронный порядковый номер устройства (ESN), международный идентификатор абонента мобильной связи (IMSI), информацию об аутентификации безопасности и шифровании, временную информацию, имеющую отношение к локальной сети, список служб, к которым имеет доступ пользователь и два пароля (пароль с персональным идентификационным номером

35 (ПИН) для обычного использования и пароль PUK, предназначенный для разблокирования). Как очевидно для специалистов в данной области техники при рассмотрении ими настоящих чертежей, спецификаций и пунктов формулы изобретения, другая информация может быть поддержана в памяти идентификации устройства в зависимости от типа устройства, его основного сетевого типа, оператора домашней

40 мобильной сети и т.д.

[0029] У переносных устройств связи может быть две подсистемы: (1) «беспроводная подсистема», обеспечивающая возможность передачи и другого применения данных, что в настоящее время стало совершенно обычным для пользователей мобильных телефонов, и (2) «защищенная транзакционная подсистема», которая может также быть

45 названа «платежной подсистемой». Защищенная транзакционная подсистема должна содержать элемент безопасности и связанное программное обеспечение устройства, предназначенное для связи с системами управления и регистрации, а также обращенный к клиенту интерфейс для использования безопасных данных и управления этими

данными, сохраняемыми в защищенном элементе. Совершенно понятно, что эта защищенная транзакционная подсистема будет предпочтительно содержать элемент безопасности, подобный (если не идентичный) элементу, описанному как часть Глобальной Платформы 2.1.X, 2.2 или 2.2.X (www.globalplatform.org). Элемент безопасности был выполнен как специализированная, отдельная физическая память, используемая для обычной в этой области техники практики хранения данных дорожки платежной карточки, используемых в обычной для этой области техники торговой точке; кроме того, другие безопасные идентификационные данные, которые могут храниться в элементе безопасности, включают идентификационные данные личного жетона работника (средства управления доступом на предприятии), основанные на использовании карточек системы доступа в отель и в другие места и транзитные идентификационные данные.

Оператор мобильной связи

[0030] Каждое из переносных устройств связи подсоединено к по меньшей мере одному оператору мобильной связи. Оператор мобильной связи обычно предоставляет физическую инфраструктуру, поддерживающую услуги беспроводной связи, применение данных и безопасную транзакционную подсистему через множество вышек сотовой связи, которые выполняют связь с множеством переносных устройств связи в пределах соответствующей ячейки каждой вышки сотовой связи. В свою очередь, вышки сотовой связи способны быть в состоянии действующей связи с логической сетью оператора мобильной связи, обычными аналоговыми телефонными линиями и Интернетом, чтобы передавать сообщения и данные в пределах собственной логической схемы оператора мобильной связи, а также во внешние сети, включая сети других операторов мобильной связи. Операторы мобильной связи обычно оказывают поддержку одному протоколу и одной технологии связи или большему количеству протоколов и технологий связи, включая, но не ограничиваясь этим, глобальную систему для мобильной связи (GSM), третье поколение мобильных сетей (3G), четвертое поколение мобильных сетей (4G), множественный доступ с кодовым разделением каналов (CDMA), множественный доступ с временным разделением каналов (TDMA), протокол пользовательских дейтаграмм (UDP), протокол управления передачей / Протокол Интернета (TCP/IP), службу коротких сообщений (SMS), общую службу пакетной радиосвязи (GPRS), протокол беспроводного доступа (WAP), сверхширокую полосу пропускания (UWB), протокол IEEE 802.16 глобальной совместимости для микроволнового доступа (WiMax), протокол SIP/RTP или любой протокол из множества других протоколов беспроводной связи, предназначенных для связи с переносными устройствами связи.

Розничная подсистема

[0031] В настоящее время стандартный подход в торговых точках состоит в использовании соединенной с протоколом Интернета платежной системы, обеспечивающей возможность обработки транзакций финансовых инструментов дебета, кредита, предварительной оплаты и дарения, поступающих от банков и провайдеров торговых услуг. При проведении действующей карточки с магнитной дорожкой через устройство магнитного считывания в кассовом терминале, происходит передача данных карточки в кассовый терминал торговой точки и их использование для подтверждения денежных средств банком, выдавшим карточку. Этот кассовый терминал торговой точки начал содержать бесконтактные устройства считывания с карточек как аксессуаров, обеспечивающие возможность представления данных платежной карточки через радиочастотный интерфейс вместо магнитного считывающего устройства. Передача данных на считывающее устройство через радиочастотный интерфейс

происходит в соответствии со стандартом ISO 14443 и посредством платежных приложений собственной разработки, таких как PayPass и Paywave, передающих данные бесконтактной карточки с карточки и в будущем, с мобильного устройства, содержащего платежную подсистему.

- 5 [0032] Кассовый терминал 75 в розничной торговой точке может быть соединен с торговой платежной сетью посредством беспроводной или проводной связи. Эта сеть кассовых терминалов может быть подключена к Интернету в дополнение к локальным сетям (локальная сеть), глобальным сетям (WAN), прямым подключениям, например, через порт универсальной последовательной шины (USB), другим формам машинно-
10 читаемых сред, или к любым комбинациям вышеуказанного. Во взаимосоединенном наборе локальных сетей, включая сети, основанные на различных архитектуре и протоколах, маршрутизатор действует в качестве средств соединения между локальными сетями, обеспечивая возможность пересылки сообщений из одной сети в другую. Кроме того, коммуникационные каналы в пределах локальной сети обычно содержат
15 скрученную проводную пару или коаксиальный кабель, в то время как коммуникационные каналы между сетями могут использовать аналоговые телефонные линии, полностью или частично выделенные цифровые линии, включая линии T1, T2, T3 и T4, цифровые сети с интеграцией услуг (ISDNs), цифровые абонентские линии (DSLs), беспроводные каналы, включая спутниковые линии, или другие
20 коммуникационные каналы, известные специалистам в данной области техники. Кроме того, удаленные компьютеры и другие соответствующие электронные устройства могут быть удаленным образом соединены или с локальными сетями или с глобальными сетями посредством модема и временного телефонного канала. В основном сеть кассовых терминалов может использовать любой способ связи, обеспечивающий
25 возможность перемещения информации между кассовыми терминалами и провайдерами финансовых услуг с целью подтверждения, предоставления разрешения и в конечном счете проведения финансовых транзакций в кассовом аппарате для оплаты через тех же самых провайдеров финансовых услуг.

Оконечный интерфейс управления системой

- 30 [0033] Система содержит окончный интерфейс управления системой. Как показано на фиг. 1B, окончный интерфейс 300 управления системой соединен с розничной подсистемой (см. кассовый терминал 75), защищенной транзакционной подсистемой 310 (состоящей из одного провайдера финансовых услуг или большего их количества) и с множеством переносных устройств 50 связи через инфраструктуру по меньшей мере
35 одного оператора мобильной связи. Оконечный интерфейс 300 управления системой содержит сервер, функционально связанный с одним клиентским устройством или большим количеством таких устройств. Сервер также имеет функциональную связь с подсистемой 75 оператора розничной торговли, защищенной транзакционной подсистемой 310 и с одним переносным устройством 50 связи или с большим
40 количеством таких устройств. Любой тип канала передачи речи может быть использован совместно с настоящим изобретением, включая, но не ограничиваясь этим, голосовую связь по IP-протоколу (VoIP).

- [0034] Сервер окончного интерфейса 300 управления системой может содержать один компьютер общего назначения или большее количество таких компьютеров,
45 которые выполняют процедуры и функции, необходимые для работы бэк-офиса системы последовательно или параллельно на одном и том же компьютере или по локальной или по глобальной сети, распределенной на множество компьютеров, и могут даже быть размещены «в облаке» (предпочтительно с выполнением условия достаточной

безопасности). Компьютер(-ы), представляющий(-ие) собой сервер, может(-ут) быть управляем(-ы) операционной системой Linux, Windows®, Windows CE, Unix или операционной системой, основанной на Java®, и многими другими операционными системами. Сервер оконечного интерфейса управления системой функционально связан с запоминающим устройством большого объема, хранящим код программы и данные. Данные могут содержать одну базу данных или большее количество таких баз, текст, электронную таблицу, общий указатель, файл и т.п., которые могут быть сконфигурированы для поддержания и хранения базы знаний, идентификаторов пользователей (электронный порядковый номер устройства, международный идентификатор абонента мобильной связи, пароль с персональным идентификационным номером, номер телефона, адрес электронной почты / IM - адрес, информация о счете и т.п.).

[0035] Сервер оконечного интерфейса управления системой может поддерживать систему сопровождения клиентов, предназначенную для обеспечения возможностей подключения и распределения трафика вызова через клиентские компьютеры в центре работы с клиентами. В предпочтительном подходе, при использовании возможностей подключения канала голосовой связи по IP-протоколу, система сопровождения клиентов представляет собой систему управления контактами/сопровождения клиентов, продаваемую компанией Contactual, Inc. из Редвуд-Сити, Калифорния. Система Contactual представляет собой стандартная систему управления отношениями с клиентами для основанного на голосовой связи по IP-протоколу телефонного информационного центра работы с клиентами, который также создает гибкость при работе со связанными с обслуживанием вопросами при наличии одновременных платежей и связанных с сотовой связью проблемами обслуживания. Как совершенно ясно специалистам в данной области техники, имеющим настоящее описание, чертежи и пункты формулы изобретения, другие системы сопровождения клиентов могут быть использованы в пределах настоящего изобретения, например, система Salesforce (компания Salesforce.com, inc. из Сан-Франциско, Калифорния) и система Novo (компания Novo Solutions, Inc. из Вирджиния-Бич, Вирджиния).

[0036] Сервер оконечного интерфейса управления системой также поддерживает сервер 2010 выпуска, базу 2011 данных однозначной идентификации пользователя, базу 2012 данных о географическом местоположении торговых точек и прогнозный модуль 2015 транзакции. Эти элементы будут рассмотрены ниже в описании.

[0037] Каждый клиентский компьютер, связанный с сервером оконечного интерфейса управления системой, содержит сетевое интерфейсное устройство, графический интерфейс пользователя и возможности голосовой связи, соответствующие каналу(-ам) передачи речи, поддерживаемому сервером центра работы с клиентами, таким как голосовая связь по IP-протоколу. Каждый клиентский компьютер может запрашивать сведения о состоянии и подсистемы сотовой связи и защищенной транзакционной подсистемы переносного устройства связи. Сведения об этом состоянии могут содержать содержимое программной памяти и базовую производительность переносного устройства связи, компоненты беспроводной связи ближнего радиуса действия: основная полоса, антенна беспроводной связи ближнего радиуса действия, состояние и идентификация элемента безопасности.

Платежная подсистема

[0038] Как показано на фиг. 2, каждое переносное устройство 50 связи может содержать кошелек 160 разового платежа, платежные библиотеки 110, элемент 120 безопасности, основную полосу беспроводной связи ближнего радиуса действия (или

радиочастотной связи), платежную подсистему 150 (то есть хранилище 115 безопасных данных и элемент 120 безопасности) и диагностические средства 170. Кошелек 160 разового платежа представляет собой компьютерное приложение, обеспечивающее любому переносному устройству связи возможность запрашивать и эмулировать идентификационные данные (например, данные карточки, купона, управления доступом и билета) вместе с основной полосой беспроводной связи ближнего радиуса действия/ радиочастотной связи, которые загружены в устройство 50 (предпочтительно в платежную подсистему 150) для временного использования. Это приложение может также быть реализовано на телефонах с обычными функциями (не смартфонах) при использовании протокола беспроводного доступа WAP, системы J2ME RTE и/или канала передачи коротких сообщений вместо приложения смартфона. Как будет описано ниже более подробно, наиболее предпочтительно, чтобы идентификационные данные были основаны на беспроводной связи ближнего радиуса действия, но они могут быть основаны на радиочастотной идентификации, двумерном штрихкоде или на арабских цифрах.

[0039] Платежные библиотеки 110 использованы кошельком 160 разового платежа для управления элементом 120 безопасности (и выполнения служебных операций на этом элементе), оконечным интерфейсом 300 управления системой и для выполнения беспроводного обеспечения через передатчик передачи данных (включая его канал коротких сообщений) на устройстве 50. Совершенно понятно, что беспроводная передача данных будет зашифрована некоторым способом и ключ шифрования будет развернут в обслуживающем модуле карточки, который функционально связан с переносным устройством 50 связи и с платежной подсистемой 150. В одном варианте реализации настоящего изобретения модуль обслуживания карточек функционально связан с кошельком 160 разового платежа (выполненным, как описано ниже, в виде стороннего приложения) и с платежной подсистемой 150. Модуль обслуживания карточек обычно осуществляет управление доступом к данным, хранимым в подсистеме 150 платежей, и управляет функцией(-ями), которую(-ые) каждому приложению разрешено провести с платежной подсистемой 150. В одном варианте реализации настоящего изобретения модуль обслуживания карточек проверяет автора/эмитента каждого стороннего приложения, используемого на переносном устройстве связи (как в целом описано ниже). Подсистема 150 платежей может быть использована для хранения учетных данных, таких как данные временной карточки разового платежа в дополнение к данным другой платежной карточки(-рт), купона, управления доступом и данным билета (например, данным билета на перевозку, данным билета на концерт и т.д.). Некоторые из этих типов идентификационных данных могут быть добавлены к платежной подсистеме и платежным библиотекам в зависимости от обстоятельств.

[0040] Хранилище 115 безопасных данных обеспечивает защищенное хранение на переносном устройстве 50 связи. Различные уровни безопасности могут быть обеспечены в зависимости от природы данных, предназначенных для хранения в хранилище 115 безопасных данных. Например, хранилище 115 безопасных данных может просто быть защищено паролем на уровне операционной системы устройства 50. Как известно, в этих операционных системах пароль может быть простым алфавитно-цифровым или шестнадцатеричным кодом, хранящимся где-нибудь на устройстве 50. В качестве альтернативы предпочтительно, чтобы данные в хранилище 115 безопасных данных были зашифрованными. Однако более вероятно, что хранилище 115 безопасных данных будет образовано как виртуальный элемент безопасности таким образом, как описано в заявке на патент, рассматриваемой одновременно с настоящей заявкой и

принадлежащей правопреемнику настоящей заявки, названной «Система и способ для обеспечения виртуального элемента безопасности на переносном устройстве связи» (заявка на патент США №13/279147, поданная 21 октября 2011 г.), содержание которой полностью включено в настоящую заявку посредством ссылки.

5 Разовый платеж через смартфон

[0041] Поскольку некоторые кассовые терминалы не принимают платежи по беспроводной связи ближнего радиуса действия и у некоторых пользователей нет установленных счетов беспроводной связи ближнего радиуса действия, настоящее изобретение обеспечивает любому переносному устройству связи возможность
10 проводить в высокой степени безопасные электронные платежи в торговых точках, которые принимают обычные электронные платежи посредством обычных кассовых терминалов.

[0042] Для использования системы для разового платежа оператору розничной торговли пользователь должен загрузить приложение для кошелька разового платежа
15 и иметь по меньшей мере один открытый счет в определенном банке. Пользователь должен также зарегистрировать по меньшей мере один счет в эмитенте 310 разового платежа (который может также быть определенным банком). Кроме того, пользователь должен также иметь службу мобильных данных для своего смартфона (или переносного устройства 50 связи).

[0043] Кошелек 160 разового платежа может в некоторой степени снять сложности, связанные с хранением, обслуживанием и использованием идентификационных данных, вследствие временного характера идентификационных данных и их комбинации с подтверждением о географическом местоположении. Среди возможных действий, которые могут быть контролируемы кошельком 160 разового платежа, присутствуют
25 действия, связанные с:

а) управлением кошельком (например, установить, сбросить или активировать код-пропуски кошелька; получить URL (унифицированный указатель ресурса) - адрес сервера беспроводного сообщения; выполнить беспроводную регистрацию реестра; установить время платежа; увеличить время платежа; установить карточку по
30 умолчанию; создать список эмитентов, провести аудит памяти; определить элемент безопасности для хранения идентификационных данных; обновить состояние кошелька);

б) управлением идентификационными данными (например, добавить идентификационные данные; рассмотреть подробности идентификационных данных; удалить идентификационные данные; активировать идентификационные данные (для
35 погашения/оплаты); деактивировать идентификационные данные; заблокировать/разблокировать идентификационные данные; запросить доступ к код-пропуску; получить изображение идентификационных данных; установить код-пропуск доступа); и

с) управлением элементом безопасности (например, получить идентификационные данные; обновить идентификационные данные; обновить метаданные; удалить
40 идентификационные данные; заблокировать/разблокировать кошелек; заблокировать/разблокировать элемент безопасности).

[0044] Фиг. 3А-3В совместно иллюстрируют один потенциальный вариант реализации (с различными потенциальными альтернативами) для последовательности операций получения и использования идентификационных данных для выполнения разового
45 платежа при использовании кошелька 160 разового платежа. Пользователь может войти в физический розничный магазин со своим смартфоном (то есть с переносным устройством 50 связи) и как обычно приступить к своим покупкам. При наличии кошелька 160 разового платежа, загруженного в смартфон 50 пользователя, когда

пользователь готов заплатить при выходе из физического розничного магазина, пользователь может использовать свой смартфон для оплаты даже через обычную систему посредством открытия приложения смартфона, предназначенного для этого.

[0045] Пользователь подходит к кассовому терминалу 75, открывает кошелек 160 разового платежа на смартфоне 50, вводит пароль пользователя/ код-пропуск через интерфейс пользователя на экране разового платежа (см. фиг. 5). Кошелек 160 разового платежа отправляет код-пропуск пользователя и географические координаты места (выработанные службой 165 идентификации местоположения, фиг. 2) на сервер 2010 выпуска (фиг. 4). В одном варианте реализации настоящего изобретения кошелек 160 разового платежа может также обеспечить пользователю возможностью передавать предполагаемый объем предстоящего платежа на сервер 2010 выпуска до выработки временной информации о платежной карточке. Посредством введения информации относительно предполагаемого объема разового платежа в последовательность операций подтверждения может быть обеспечена дополнительная безопасность в отношении разового кода.

[0046] Сервер 2010 выпуска проверяет код-пропуск (например, используя базу 2011 данных однозначной идентификации пользователей). Получение правильного кода-пропуска указывает системе, что пользователь будет проводить платеж в течение короткого заранее определенного промежутка времени (порядка нескольких минут, причем при определенных обстоятельствах этот промежуток может быть увеличен). Сервер 2010 выпуска использует географические координаты места, полученные от переносного устройства 50 связи, для определения вероятной торговой точки и ищет подробные описания кассового терминала торговой точки в базе данных, функционально связанной с сервером 2010 выпуска (например, в базе 2012 данных с коллекцией данных о географическом местоположении торговых точек). В частности, на основании полученной информации о географическом местоположении сервер 2010 выпуска выполняет запрос к базе данных для определения, какой бесконтактный кассовый терминал торговой точки установлен (или вероятно, может быть установлен) в месте расположения пользователя. В предпочтительном варианте реализации настоящего изобретения переносное устройство 50 связи может также выводить на дисплей список следующих наиболее вероятных розничных магазинов (например, последующие верхние пять магазинов), где переносное устройство 50 связи может быть размещено (см., например, фиг. 6А). На основании определенных местоположений и/или кассовом терминале торговой точки модуль обслуживания карточек переносного устройства 50 связи конфигурирует платежную систему 150 с форматами данных и другими бесконтактными данными торговой точки, характерными для этого местоположения и/или кассового терминала, таким образом, что устройство 50 поддержано или оптимальное представление карточки, купона, билета или эмуляции управления доступом... Система может также показать пользователю новые инструменты в виде карточек, доступных для этого географического местоположения, которые пользователь еще не загрузил в платежные библиотеки 110. В некотором варианте реализации настоящего изобретения система может загрузить необходимые библиотеки.

Сервер 2010 выпуска содержит базу данных (например, базу 2012 данных с коллекцией данных о географическом местоположении торговых точек) для всех торговых точек, принимающих электронные платежи, которая может содержать данные о местоположении торговых точек, идентификационный номер торговой точки, используемый при обычных электронных платежах, обычные схемы платежей,

одобренные в каждом местоположении торговой точки, и возможности оборудования кассовых терминалов в каждом местоположении торговой точки (см. таблицу 1 ниже). Хотя база 2012 данных с коллекцией данных о географическом местоположении торговых точек описана как содержащаяся в пределах сервера 2010 выпуска или иным образом составляющая его часть, предположено, что база 2012 данных с коллекцией данных о географическом местоположении торговых точек может содержаться в пределах переносного устройства 50 связи, эмитента 310 или составлять их часть или быть связанной с ними или может быть размещена отдельно.

Таблица 1

Примеры торговых точек и информации о разовом платеже					
Название торговой точки	Месторасположение торговой точки (данные глобальной системы позиционирования (широта/долгота))	Адрес местоположения торговой точки	Обычный идентификационный номер торговой точки	Обычный способ платежа	Возможности оборудования
Grocery Land	37,48° с.ш., 122,24° з.д.	100 Marine Parkway Suite 400 Redwood City, CA 94065	XQ24MZ122A	Штрихкод	Лазерный сканер
Appliance Land	37,48° с.ш., 122,24° з.д.	110 Marine Parkway Redwood City, CA 94065	YF234XY302	Трехмерный штрихкод	Считывающее устройство трехмерного штрихкода
Must Buy	37,48° с.ш., 122,24° з.д.	120 Marine Parkway Redwood City, CA 94065	MN343D	Беспроводная связь ближнего радиуса действия	Считывающее устройство беспроводной связи ближнего радиуса действия

[0047] Сервер 2010 выпуска затем вырабатывает временную платежную карточку разового использования и передает данные временной платежной карточки и идентификационные данные вероятной торговой точки переносному устройству 50 связи беспроводным способом. Эта информация о временной платежной карточке может быть отформатирована в режиме реального времени при использовании обычных стандартов и практических методик, применяемых в отрасли обычных электронных платежей, включая персональный номер счета, идентификационный номер эмитента, стандарт ISO/IEC 7812 (относящийся к идентификации эмитентов посредством использования идентификационного номера эмитента (UN) для работы при международном, межотраслевом и/или внутриотраслевом обмене), стандарт ISO/IEC 7813 (относящийся к структуре данных и к содержимому магнитных дорожек, используемых для первоначальных финансовых транзакций) и форматирование по протоколу ISO 8583 (который представляет собой протокол обмена бизнес-сообщениями, основанный на собственном стандарте).

[0048] В одном предпочтительном варианте реализации настоящего изобретения кошелек 160 разового платежа форматирует временную платежную карточку на основании возможностей переносного устройства 50 связи, а также возможностей кассового терминала 75 торговой точки. Информация о временной платежной карточке может также быть отформатирована в разных форматах, чтобы предоставить пользователю опции, которые могут быть предоставлены кассиру торговой точки. На фиг. 7А и 7В показаны два из возможных типов кодов разового платежа, которые могут быть переданы в переносное устройство 50 связи. На фиг. 7А показан код разового платежа в виде двумерного штрихкода. Как должно быть понятно специалистам в данной области техники, этот штрихкод может быть трехмерным кодом или кодом типа QR. На фиг. 7В показан код разового платежа в виде числового кода, который может быть последовательностью 16 цифр или, при необходимости, последовательностью другой длины.

[0049] Один формат, посредством которого информация о временной платежной

карточке может быть представлена на дисплее смартфона, представляет собой совместимый номер согласно стандарту ISO/IEC 7813 (то есть основной номер держателя банковской карточки (PAN)), который клерк в торговой точке вводит вручную в кассовый терминал торговой точки. Другой формат, посредством которого данные временной платежной карточки могут быть представлены на дисплее смартфона, представляет собой штрихкод (стандарт ISO/IEC 15426-1), двумерный штрихкод (стандарт ISO/IEC 15426-2), код типа QR (стандарт ISO/IEC 18004:2006), или другие такие аналогичные способы, которые передают данные в виде символов Американского стандартного кода для обмена информацией (ASCII) с последующим захватом этих данных сканером кассового терминала торговой точки. Еще один формат, посредством которого могут быть представлены данные временной платежной карточки, может быть реализован посредством режима равноправных узлов в беспроводной связи ближнего радиуса действия (стандарт ISO/IEC 18092), эмуляции тегов в беспроводной связи ближнего радиуса действия (формат обмена данных в беспроводной связи ближнего радиуса действия (NDEF), стандарт ISO 14443 и система Felica), или режима эмуляции карточки беспроводной связи ближнего радиуса действия (эмуляция карточки по стандарту ISO 14443) или режимов радиочастотной идентификации.

[0050] Для обеспечения дополнительной безопасности данные временной платежной карточки исчезают по прошествии короткого заранее определенного промежутка времени, например, двух (2) минут. Это время может быть увеличено по желанию эмитента. Следует иметь в виду, что было бы предпочтительно время меньше 30 минут, или даже меньше 20 минут, или даже 10 минут. При необходимости могут быть использованы и/или запрограммированы другие времена истечения срока.

[0051] Переносное устройство 50 связи получает временные идентификационные данные вероятной торговой точки и информацию об эмуляции от сервера 2010 выпуска. В предпочтительном варианте реализации настоящего изобретения переносное устройство 50 связи подтверждает, что вероятная торговая точка была правильно выбрана из базы 2012 данных. В одном подходе, показанном в связи с фиг. 6, переносное устройство связи просит пользователя подтвердить местоположение. В показанном примере интерфейс пользователя спрашивает, представляет ли собой данное место магазин Grocery Land. При нахождении пользователя, как показано на фиг. 1А, в магазине Grocery Land пользователь должен нажать кнопку «да» на фиг. 6. При выборе системой неправильного оператора розничной торговли система может предложить альтернативные варианты для установления правильного оператора розничной торговли. Например, фиг. 6А показывает выведение на экран списка потенциальных торговых точек, близких к местоположению пользователя в примере, где разовые идентификационные данные были затребованы изнутри того объекта, который сервер 2010 выпуска распознал в качестве торгового центра (или другой высокоплотной группировки торговых точек). Как совершенно ясно специалистам в данной области техники, имеющим настоящее описание, чертежи и пункты формулы изобретения, список соседних торговых точек не должен быть ограничен торговыми точками в пределах одного торгового центра. Альтернативные варианты могут быть выбраны из других операторов розничной торговли, размещенных географически близко к географическому положению, полученному сервером. Как дополнительно должно быть ясно, альтернативные варианты могут быть представлены окончательному пользователю в виде выпадающего меню или списка.

[0052] В варианте реализации настоящего изобретения, где пользователь использует портативное устройство 50 для подтверждения торговой точки, подтверждение

вероятной торговой точки может быть получено посредством сервера 2010 выпуска. При неправильной идентификации вероятной торговой точки сервер выпуска может выдать новую информацию об эмуляции к переносному устройству 50 связи. При известной вероятной торговой точке прогнозный модуль 2015 транзакции сервера 2010
 5 выдачи передает идентификационный номер для этой вероятной торговой точки, однозначный идентификатор пользователя, связанный с переносным устройством 50 связи, токен разового использования, выработанный для транзакции, и время истечения срока в межсетевой шлюз 2020 с отображением проверки правильности.

[0053] Межсетевой шлюз 2020 с отображением проверки правильности может быть
 10 физически размещен в банке, эмитенте 310 или в сети процессора платежей и может быть развернут или как служба или как подсистема, установленная и интегрированная в обычных процессорах транзакций, расчетных схемах, финансовых учреждениях и в других объектах. После получения данных от прогнозирующего модуля 2015 транзакции полученные данные хранят в базе данных, связанной с межсетевым шлюзом с
 15 отображением проверки правильности. При наличии таких данных временные данные могут быть связаны с данными обычной карточки, ранее связанными с однозначным идентификатором пользователя. В той степени, в которой существуют такие ассоциации между обычной карточкой и однозначным идентификатором пользователя, они могут быть созданы эмитентами 310 или даже пользователем в электронной транзакции
 20 непосредственно между переносным устройством 50 связи и межсетевым шлюзом 2020 с отображением проверки правильности, управляемым оконечным интерфейсом 300 управления системой.

[0054] В предпочтительном варианте реализации прогнозный модуль 2015 транзакции отправляет данные в межсетевой шлюз 2020 с отображением проверки правильности
 25 в по существу тот же самый момент времени, когда происходит передача информации разового использования об идентификационных данных в переносное устройство 50 связи. При таком подходе межсетевой шлюз 2020 с отображением проверки правильности может опережать пользовательскую транзакцию от кассового терминала 75 торговой точки через платежную сеть торговой точки. В частности, в таком варианте
 30 реализации изобретения межсетевой шлюз 2020 с отображением проверки правильности может использовать время между получением данных от прогнозного модуля 2015 транзакции и получением транзакции от кассового терминала 75 розничной торговой точки для извлечения сохраненных данных из большой базы данных и переноса их в запоминающее устройство, которое обеспечит более быстрый доступ (по сравнению
 35 со временем доступа из большой базы данных) и проведения сравнения между сохраненными данными и данными, полученными из торговой платежной сети. При таком подходе добавление этой дополнительной операции проверки в межсетевом шлюзе 2020 с отображением проверки правильности создает меньшую задержку, чем задержка, которая, возможно, в противном случае была бы определена необходимостью
 40 найти и извлечь данные для этого сравнения после получения транзакции от кассового терминала 75.

[0055] Возвратившись к пользователю отметим, что после получения портативным устройством 50 временных идентификационных данных и информации об эмуляции пользователь может затем коснуться экрана смартфона 50 или иным образом
 45 активировать его в кассовом терминале 75 с включенной одноранговой беспроводной связью ближнего радиуса действия, что вынуждает переносное устройство связи эмулировать идентификационные данные с кодом разового платежа, используя протокол эмуляции, предоставленный сервером. Следует иметь в виду, что этот код может быть

визуально «эмулирован» на экране переносного устройства 50 связи. Поскольку данные временной платежной карточки могут быть предоставлены в обычных форматах, данные временной платежной карточки могут быть акцептованы обычным кассовым терминалом 75 торговой точки.

5 [0056] Кассовый терминал 75 торговой точки затем обрабатывает данные временной платежной карточки через обычную платежную сеть торговой точки, как будто это были стандартные кредитные или дебетовые идентификационные данные. Однако, поскольку данные временной платежной карточки используют идентификационные номера эмитента (стандарт ISO/IEC7812), которые были зарегистрированы и отображены
10 к провайдеру системы разового платежа, выступающего в качестве эмитента, эти данные будут направлены в межсетевой шлюз 2020 с отображением проверки правильности через платежную сеть торговой точки. При получении данных межсетевым шлюзом 2020 с отображением проверки правильности до окончания срока истечения для временных идентификационных данных и от предполагаемой вероятной торговой
15 точки межсетевой шлюз 2020 с отображением проверки правильности может одобрить транзакцию (при наличии денежных средств и т.д.). Межсетевой шлюз 2020 с отображением проверки правильности может также сравнить способ, посредством которого данные платежной карточки были введены в кассовый терминал 75 торговой точки (обычная определенная группа разрядов по стандарту ISO 8583), со способом,
20 посредством которого данные временной карточки были поданы на мобильный телефон (например, числовой код, штрихкод, беспроводная связь ближнего радиуса действия).

[0057] И снова, при согласовании всех требуемых характеристик (например, временного кода, времени выполнения, идентификатора торговой точки и типа эмуляции) межсетевой шлюз с отображением проверки правильности может вернуть
25 подтверждение в торговую точку с кодом одобрения через платежную сеть торговой точки. Кассовый терминал 75 торговой точки получает авторизацию (то есть подтверждение платежной акцептации с кодом одобрения), распечатывает чек и пользователь покидает магазин с новыми купленными им товарами.

[0058] В качестве альтернативы, после проверки информации о временной платежной карточке (включая данные о времени и идентификатор вероятной торговой точки)
30 система обладает опцией передачи запроса на выполнение эквивалентной платежной транзакции в эмитент 310 для одобрения транзакции. Это известно как выполнение компенсационной платежной транзакции. Таким образом, пользователь и торговая точка получили бы платежное подтверждение со счета обычной банковской кредитной
35 или дебетовой карточки потребителя, вместо номера временной карточки. В частности, после подтверждения разового акта платежа межсетевой шлюз 2020 с отображением проверки правильности заменяет данные платежа по обычной карточке в данных транзакции, которые затем передают в системы авторизации эмитента 310 вместе со стандартной информацией о проводимой на кассовом терминале транзакции (например,
40 идентификатор торговой точки и сумму транзакции) и, в некоторых примерах реализации настоящего изобретения, с указанием на то, что транзакция использовала проверенные идентификационные данные разового использования (чтобы показать дополнительную меру безопасности). Эмитент 310 рассмотрит данные обычной карточки и информацию о транзакции для принятия решения об авторизации транзакции способом,
45 общеизвестным в данной области техники, возможно, вместе с информацией, что транзакция имеет отмеченную выше дополнительную защиту. Авторизацию эмитента отсылают назад в кассовый терминал 75 торговой точки через обычный существующий канал обработки.

[0059] Этот подход к идентификационным данным разового использования может быть использован для многих различных типов сценариев подтверждения идентификационных данных: платежи по кредитной карточке и дебетовой карточке, подарочная карточка, карточка постоянного покупателя, купоны и предложения, управление доступом и любая другая среда, где пользователь предоставляет идентификационные данные для проверки в физической среде.

[0060] Хотя функциональные возможности могут быть объединены в пределах кошелька 160 разового платежа, интерфейс пользователя может быть снабжен пользовательским интерфейсом кошелька, а беспроводное обеспечение и управление подсистемой защищенных платежей (и доступ к ней) поддерживаются функциональными возможностями модуля обслуживания карточек. Лежащий в основе интерфейса пользователя модуль обслуживания карточек содействует беспроводному обеспечению, управлению элементом безопасности и непосредственному ключевому обмену между модулем обслуживания карточек на мобильном устройстве 50 пользователя и соответствующим сервером эмитента (для кошелька 160 разового платежа, который может быть сервером 2010 выпуска) зашифрованным способом, как было ранее известно в этой области техники.

Приложение, подтверждающее разовый платеж, как стороннее приложение

[0061] Как показано на фиг. 8А-8В, кошелек 160 разового платежа может быть развернут как одно из многих надежных приложений 200 третьей стороны. Модуль обслуживания карточек проверяет статус надежности любого приложения 200 перед тем, как этому приложению будет предоставлен доступ к элементу 120 безопасности (или к хранилищу 115 безопасных данных и даже предпочтительно к репозитарию метаданных, который хранит, помимо другого, данные изображения карточки и любые рельефные данные карточки) на переносном устройстве 50 связи, для просмотра, выбора и/или изменения безопасных данных, хранимых в подсистеме 150 платежей. Эта проверка может быть выполнена посредством получения доступа к локальной базе данных авторизации разрешенных или надежных приложений. В предпочтительном подходе локальная база данных авторизации сотрудничает с удаленной базой данных авторизации, связанной с одним сервером или большим количеством серверов, связанных с окончательным интерфейсом 300 управления системой.

[0062] На фиг. 10 показана блок-схема одной потенциальной реализации одной потенциальной комбинации локальных и удаленных баз данных авторизации, предназначенной для улучшения безопасности модуля обслуживания карточек, элемента 120 безопасности и подсистемы 150 платежей. Как показано на фиг. 10, регистр текущего счета пользователя (или регистр счета пользователя) может быть связан с сервером (или иначе развернут в глобальной сети). Регистр текущего счета пользователя может хранить идентификацию элемента 120 безопасности, размещенного в портативном устройстве 50 каждого пользователя. Записи в регистре текущего счета пользователя могут быть добавлены для каждого пользователя в любой точке последовательности операций.

[0063] База данных регистра эмитента представляет собой базу данных одобренных эмитентов. Идентификатор эмитента уникален для каждого типа идентификационных данных. Другими словами, при наличии у банка многих типов идентификационных данных (например, дебетовые карточки, кредитные карточки, дисконтные карточки и т.д.) каждый тип идентификационных данных должен иметь свой собственный идентификатор эмитента (например, I-BofA-II). При предпочтительном подходе идентификаторы эмитента для многих типов идентификационных данных должны

иметь некоторые общие элементы, чтобы указывать, что идентификационные данные по меньшей мере связаны друг с другом (например, I-BofA-I). Таким образом, приложения, исходящие от одного эмитента, могут совместно использовать данные с другим приложением из того же самого «расширенного» эмитента. В предпочтительном подходе модуль обслуживания карточек может быть упрощен посредством требования, чтобы даже интерфейс пользователя кошелька (который «поставлен вместе с системой») имел идентификатор эмитента (так же как идентификатор приложения и токен компиляции).

[0064] «Регистр приложения» представляет собой базу данных приложений (главным образом, от третьей стороны), которые были предварительно одобрены провайдером операционной системы. Как и регистр текущего счета пользователя, «Регистр приложений» и база данных «регистра эмитентов» поддерживаются на стороне сервера (или иным образом, в глобальной сети) в функциональной ассоциации с приложением для разового платежа. Как очевидно для специалистов в данной области техники, прочитавших настоящее описание, различные регистры могут быть реализованы в отдельных базах данных или в одной объединенной базе данных. При инициировании кошелька 160 и, предпочтительно, с по существу регулярными временными интервалами после этого (например, ежедневно), данные, хранящиеся в регистре приложения для кошелька 160 разового платежа, распределены на устройства с кошельком, который будет храниться локально.

[0065] Как показано на фиг. 10, регистр приложения может содержать, вместе с другой информацией, идентификатор приложения, идентификатор эмитента и идентификатор или токен компиляции. Идентификатор компиляции представляет собой глобальную константу, выработанную для каждого приложения в ходе одной последовательности операций или большего количества таких последовательностей, связанных с кошельком разового платежа во время последовательности операций квалификации для определенного приложения. После его выработки определенным модулем обслуживания карточек на единственном устройстве 50, токен компиляции включен в приложение или иным образом связан с приложением. Предпочтительно, чтобы этот токен компиляции был выработан генератором псевдослучайных чисел, локальным относительно того устройства, которое использует заранее определенное начальное число, такое как идентификатор приложения, идентификатор компиляции, идентификатор эмитента или некоторую комбинацию этих идентификаторов.

[0066] При попытке пользователя квалифицировать приложение с модулем обслуживания карточек на устройстве 50, идентификатор компиляции (цифровой токен) и идентификатор приложения (цифровой идентификатор), связанные со сторонним приложением, могут быть противопоставлены парам идентификатора компиляции и идентификатора приложения, хранящимся в регистре обслуживания карточек, хранящемся на устройстве 50 (см. фиг. 10). Как очевидно для специалистов в данной области техники, прочитавших настоящее описание, те же самые пары идентификатора компиляции и идентификатора приложения также переданы другим устройствам 50, связанным с системой. При соответствии пары (идентификатор компиляции/идентификатор приложения) одной из пар, хранящихся в регистре обслуживания карточек на устройстве, идентификатор конфиденциального токена предпочтительно выработан на устройстве 50 генератором псевдослучайных чисел (например, таким, как генератор, связанный с элементом 120 безопасности и затем сохраненный вместе с парой (идентификатор компиляции/идентификатора приложения) в регистре обслуживания карточек на устройстве 50). В некоторых случаях идентификатор

компиляции может быть выбран предварительно и использован в качестве начального значения для генератора случайных чисел. Совершенно понятно, что вместо этого одна часть или большее количество частей других заранее определенных данных, связанных с регистром обслуживания карточек, могут быть предварительно выбраны в качестве начального значения. Предпочтительно, чтобы регистр обслуживания карточек был занесен в защищенную память (а не в элемент 120 безопасности, поскольку элемент 120 безопасности обладает ограниченным доступным пространством), и предпочтительно, чтобы регистр обслуживания карточек был дополнительно зашифрован с использованием стандартных способов шифрования. Идентификатор конфиденциального токена также встроен с приложение 200 на устройстве 50 (или иным способом связан с ним) вместо идентификатора компиляции, который был распределен вместе с приложением.

[0067] После загрузки кошелька 160 разового платежа в регистр обслуживания карточек (и в конфиденциальный токен, встроенный в приложение) кошелек 160 разового платежа может запускать приложение и может побуждать пользователя согласиться на доступ к специфичным для эмитента идентификационным данным, необходимым для аттестованного (или надежного) приложения. При каждом последующем запуске приложения 160 для кошелька разового платежа встроенный конфиденциальный токен и/или идентификатор приложения сравнивают с данными в регистре обслуживания карточек на устройстве. При наличии соответствия приложение полагают надежным и оно может получить доступ к подсистеме 150 платежей через модуль обслуживания карточек. Таким образом, можно заметить, что приложения 200 или интерфейс пользователя кошелька могут также быть удалены из регистра обслуживания карточек и таким образом будут отключены от доступа к платежной подсистеме и, возможно, к приложению в целом.

[0068] Модуль обслуживания карточек также предпочтительно использует операцию проверки надежного приложения для определения соответствующего уровня доступа к подсистеме, разрешенного для кошелька 160 разового платежа. Например, в одном варианте реализации настоящего изобретения приложению может быть разрешено получить доступ ко всем данным (и вывести их на дисплей), содержащимся в подсистеме 150 платежей, причем другому приложению может быть разрешено лишь получить доступ и вывести на дисплей подмножество данных, содержащихся в подсистеме 150 платежей. В еще одном варианте реализации настоящего изобретения приложению может быть разрешено лишь отправлять платеж или запросы на транзакцию к кошельку 160 разового платежа, но не может быть разрешено самостоятельно получать доступ ни к каким данным, содержащимся в подсистеме 150 платежей. В одном подходе присвоение прав доступа приложению может быть организовано следующим образом:

	Зарезервировано	Все идентификационные данные	Идентификационные данные эмитента	Собственные идентификационные данные
Прочитать	0	0 или 1	0 или 1	0 или 1
Записать	0	0 или 1	0 или 1	0 или 1
Удалить	0	0 или 1	0 или 1	0 или 1
Активировать/Деактивировать	0	0 или 1	0 или 1	0 или 1
Загрузить идентификационные данные	0	0 или 1	0 или 1	0 или 1

Эти права доступа могут быть использованы для образования 4-значного шестнадцатеричного числа в показанном выше порядке от цифры самого старшего разряда до цифры самого младшего разряда. Как показано в приведенном в качестве примера регистре обслуживания карточек на фиг. 10, эмитент I-BofA-II имеет уровень

разрешения 11111, который как полагают, может быть развернут в 00010001000100010001. Другими словами, приложение I-BofA-II может читать, записывать, удалять, активировать/деактивировать и загружать свои собственные идентификационные данные, но не расширенные идентификационные данные эмитента, не говоря уже о всех идентификационных данных. При наличии у VofA другого кода эмитента (например, I-BofA-I), оно был бы расширенным приложением эмитента. Так, при установлении уровня разрешения для приложения, связанного с идентификатором «I-BofA-II» эмитента, на значение 00100001000100100001 (или 21121 в шестнадцатеричном формате) это приложение было бы в состоянии считывать и активировать/

деактивировать идентификационные данные, связанные с обоими идентификаторами эмитента. В еще одном примере пользовательскому интерфейсу кошелька может быть задан уровень разрешения 44444 (то есть 01000100010001000100). Другими словами, интерфейс пользователя кошелька может считывать, записывать, удалять, активировать/деактивировать, и загружать все идентификационные данные. Как должно быть понятно специалистам в данной области техники, это просто примеры потенциальных полномочий, которые можно предоставлять приложениям, предполагаются и другие полномочия. Например, некоторые приложения могут обладать возможностью считывать расширенные идентификационные данные эмитента, но лишь записывать, удалять, активировать и загружать собственные идентификационные данные приложения (например, 21111, что при развертывании дает 00100001000100010001). В еще одном примере приложению могут быть предоставлены права только на активацию/деактивацию и загрузку (например, 00000000000000010001 или 00011 в шестнадцатеричном формате). В еще одном примере приложение может быть выключено без удаления из базы данных надежных приложений или регистра обслуживания карточки, но с обнулением всех прав.

[0069] В варианте реализации настоящего изобретения, где приложение 160 кошелька разового платежа конфигурировано как одно из надежных приложений третьей стороны, оно должно быть зарегистрировано для получения доступа к операции «открыть кошелек 100» (или даже к модулю обслуживания карточек). Приложение 160 кошелька разового платежа было разработано эмитентом, связанным с сервером 2010 выпуска. Затем приложение 160 кошелька разового платежа может эмулировать идентификационные данные беспроводной связи ближнего радиуса действия. В соответствии с этим приложению 160 кошелька разового платежа должен быть предоставлен уровень разрешения 11111, который можно развернуть в 00010001000100010001. Другими словами, приложение 160 кошелька разового платежа может считывать, записывать, удалять, активировать/деактивировать и загружать свои собственные идентификационные данные, но не расширенные идентификационные данные эмитента или любые другие идентификационные данные.

[0070] Предшествующее описание примеров реализации изобретения и чертежи относятся к кошельку 160 разового платежа и идентификационным данным разового платежа или к информации или данным временной платежной карточки, которые истекают по прошествии короткого заранее определенного промежутка времени. Однако понятно, что кошелек 160 разового платежа можно вместо этого полагать динамическим временным кошельком 160 и что идентификационные данные/информацию разового платежа и данные временной платежной карточки можно полагать динамическими временными идентификационными данными. Кроме того, идентификационные данные (1) могут быть «повторенными в цикле» и быть снова использованы в пределах системы другими пользователями; (2) могут иметь заранее

определенное время жизни, продолжительнее «короткого» заранее определенного промежутка времени, причем (3) такие идентификационные данные могут быть использованы для более чем просто покупки товаров. Далее предположено, что хотя предшествующее описание примеров реализации изобретения и чертежи имеют, прежде
 5 всего, отношение к кассовому терминалу 75, связанному с торговой точкой, предшествующее описание, чертежи и варианты реализации настоящего изобретения могут быть приложены ко множеству других точек с электронным управлением, например, к приемопередающим устройствам по распределению гостиничных номеров, офисным приемопередающим устройствам, приемопередающим устройствам по прокату
 10 автомобилей и т.д. Например, точки электронного управления могут содержать любую точку доступа, например кассовые терминалы, приемопередатчики с радиочастотной идентификацией, приемопередатчики штрихкода, приемопередатчики беспроводной связи ближнего радиуса действия и т.д.

[0071] В частности, идентификационные данные обычно должны быть «оплачены»
 15 эмитентом 310 или другой организацией в пределах полной большой торговой платежной системы. Как таковые, системы могут иметь в своем распоряжении лишь ограниченное количество идентификационных данных. Использование таких идентификационных данных только один раз для определенных пользователя и транзакции может привести к неоправданно высоким затратам по сравнению с системой, где платежные
 20 идентификационные данные зациклены для использования многими пользователями в неодинаковые моменты времени и, предпочтительно, в неодинаковых географических местоположениях для обеспечения дополнительной защиты от мошенничества. Например, сервер 2010 выпуска может отслеживать выпуск данных (и срок окончания их действия), связанных с идентификационными данными, в отношении первого
 25 пользователя, работающего с первым переносным устройством 50 связи, размещенным в первом географическом местоположении (например, в штате Калифорния), и после наступления даты и времени истечения срока действия этих идентификационных данных повторно присвоить эти же идентификационные данные второму пользователю, работающему со вторым переносным устройством 50 связи, размещенным во втором,
 30 не совпадающим с первым географическим местоположении (например, в штате Флорида).

[0072] Аналогичным образом идентификационные данные могут иметь более продолжительные периоды времени жизни, чтобы позволить использование
 35 идентификационных данных во множестве «торговых точек» или в других точках с электронным управлением. Например, на фиг. 9А и 9В взятый в качестве примера интерфейс пользователя кошелька показан на переносном устройстве 50 связи. Кошелек 160 может содержать множество платежных карточек и быть связан с ними (например, с карточками типа MasterCharge, Visa, Charge-It и т.д., как показано на фиг. 9А) и может дополнительно содержать множество других не связанных с платежом приложений и
 40 быть связан с ними (например, ключ от номера в отеле, офисная карточка-ключ, брелок для прокатного автомобиля и т.д., как показано на фиг. 9В). Хотя предпочтительно, чтобы период «времени жизни» был мал при продаже через кассовый терминал для усиления безопасности, совершенно понятно, что «время жизни» может быть значительно более продолжительным при ассоциации кошелька с не связанными с
 45 оплатой приложениями, такими как ключ от номера в отеле. В таком примере кошелек 160 может быть использован для открытия или закрытия номера пользователя в отеле. Таким образом, «время жизни» должно быть установлено по меньшей мере равным длительности пребывания пользователя в отеле. Точно так же время жизни может быть

установлено равным промежутку времени (при необходимости бесконечному), в течение которого пользователю устройства 50 разрешено использовать устройство 50 для получения доступа к офису или прокатному автомобилю.

[0073] Таким образом, также следует иметь в виду, что оконечный интерфейс 300 управления системой и эмитент 310 могут быть связаны с нефинансовыми услугами, чтобы разрешить использование приложений кошелька, не связанных с платежом. Например, оконечный интерфейс 300 управления системой может содержать данные, относящиеся к нефинансовым услугам (например, местоположение отеля, местоположение офиса и т.д.), и этот эмитент 310 может быть аффилирован с организациями, не связанными с платежом (например, с отелями, офисными организациями и т.д.).

[0074] Предшествующие описание изобретения и чертежи лишь поясняют и иллюстрируют изобретение, и изобретение ими не ограничено. Хотя описание выполнено в связи с определенным воплощением или вариантами реализации настоящего изобретения, многие подробности сформулированы лишь с целью иллюстрации. Таким образом, предшествующее описание просто иллюстрирует сущность изобретения. Например, изобретение может иметь другие определенные формы без отступления от его сути или существенных характеристик. Описанные конфигурации иллюстративны и не вносят ограничений. Как ясно специалистам в данной области техники, изобретение подвержено дополнительным воплощениям и вариантам реализации и некоторые из подробностей, описанных в настоящей заявке, могут быть значительно изменены без отступления от основных принципов настоящего изобретения. Следует, таким образом, иметь в виду, что специалисты в данной области техники будут в состоянии разработать различные конфигурации, которые, хотя и не описаны или показаны здесь, сохраняют принципы изобретения, не выходя за пределы его объема и сути.

(57) Формула изобретения

1. Система проверки транзакции между переносным устройством связи и точкой электронного управления с использованием динамических временных идентификационных данных, выпущенных в переносное устройство связи, при этом переносное устройство связи имеет службу, предоставляющую текущее географическое местоположение переносного устройства связи, причем система содержит:

- средство хранения информации о коде-пропуске в базе данных идентификации пользователя;
- средство приема кода-пропуска и текущего географического местоположения переносного устройства связи от переносного устройства связи;
- средство проверки кода-пропуска с использованием информации о коде-пропуске;
- средство определения, после проверки кода-пропуска, одного или более вероятных торговых точек и типа точки электронного управления в пределах одной или более торговых точек с использованием координат географического местоположения;
- средство генерирования динамических временных идентификационных данных с использованием определенного типа точки электронного управления и маршрутной информации межсетевого шлюза с отображением проверки правильности;
- средство передачи динамических временных идентификационных данных переносному устройству связи от централизованного компьютера; и
- средство предоставления прогнозной информации о транзакции системе авторизации, функционально ассоциированной с точкой электронного управления, причем прогнозная информация о транзакции включает в себя динамические временные идентификационные

данные, идентификатор торговой точки для вероятных торговых точек, идентификатор пользователя, ассоциированный с переносным устройством связи, срок истечения для динамических временных идентификационных данных и информацию, указывающую на текущее географическое местоположение переносного устройства связи; и

- 5 - средство проверки транзакции с динамическими временными идентификационными данными, которые были приняты от точки электронного управления в пределах вероятной торговой точки до срока истечения, и типом эмуляции, связанным с точкой электронного управления.

- 10 2. Система по п. 1, в которой переносное устройство связи обладает однозначной цифровой подписью, а средство проверки дополнительно проверяет связь кода-пропуска с однозначной цифровой подписью, ассоциированной с переносным устройством связи.

3. Система по п. 2, в которой средство предоставления дополнительно предоставляет однозначную цифровую подпись переносного устройства связи.

- 15 4. Система по п. 1, в которой каждая из указанных одной или более вероятных торговых точек представлена названием торговой точки и идентификационным кодом торговой точки.

- 20 5. Система по п. 1, в которой средство передачи дополнительно передает одну или более вероятных торговых точек в переносное устройство связи, причем система дополнительно содержит средства для удостоверения подтверждения одной или более вероятных торговых точек от переносного устройства связи, а средство удостоверения выбирает другую одну или более вероятных торговых точек после приема указания отсутствия соответствия.

- 25 6. Система по п. 1, в которой система авторизации дополнительно содержит межсетевой шлюз с отображением проверки правильности, соединенный с платежной сетью торговой точки, причем платежная сеть торговой точки соединена с точкой электронного управления, которая является кассовым терминалом.

7. Система по п. 6, в которой межсетевой шлюз с отображением проверки правильности включает в себя базу данных проверки правильности, содержащую динамические временные идентификационные данные и данные об обычном платеже.

- 30 8. Система по п. 7, в которой межсетевой шлюз с отображением проверки правильности функционально соединен с одним или более эмитентами, причем система дополнительно содержит средство, ассоциированное с межсетевым шлюзом с отображением проверки правильности, для замены данных об обычном платеже на динамические временные идентификационные данные в транзакции платежа до
35 отправления транзакции платежа эмитенту, ассоциированному с данными обычного платежа.

9. Система по п. 8, в которой средство проверки дополнительно включает в себя средство проверки того, что время выполнения соответствует ожидаемому значению.

- 40 10. Система по п. 9, в которой средство проверки дополнительно включает в себя средство проверки того, что динамические временные идентификационные данные являются из торговой точки, наиболее вероятным образом размещенной в текущем географическом местоположении.

- 45 11. Система по п. 1, в которой срок истечения составляет промежуток порядка нескольких минут, при этом система дополнительно содержит средство циклического повторения динамических временных идентификационных данных, причем средство циклического повторения использует текущее географическое местоположение переносного устройства связи, географическое местоположение второго переносного устройства связи и срок истечения, ассоциированный с динамическими временными

идентификационными данными, для передачи динамических временных идентификационных данных на второе переносное устройство связи после истечения срока, при размещении второго переносного устройства связи во втором несовпадающем географическом местоположении относительно текущего географического

5 местоположения первого переносного устройства связи.

12. Способ проверки транзакции между переносным устройством связи и точкой электронного управления с использованием динамических временных идентификационных данных, выпущенных в переносное устройство связи, при этом переносное устройство связи имеет службу, предоставляющую текущее географическое

10 местоположение переносного устройства связи, причем способ содержит операции:

- хранения, централизованным компьютером, информации о коде-пропуске в базе данных идентификации пользователя;

- приема кода-пропуска и текущего географического местоположения переносного устройства связи в централизованном компьютере;

15 - проверки, централизованным компьютером, кода-пропуска с использованием информации о коде-пропуске;

- на основании проверки, определения, централизованным компьютером, использования координат текущего географического местоположения вероятной торговой точки и типа точки электронного управления в пределах вероятной торговой

20 точки;

- генерирования, централизованным компьютером, динамических временных идентификационных данных с использованием определенного типа точки электронного управления и маршрутной информации межсетевого шлюза с отображением проверки правильности;

25 - передачи сгенерированных динамических временных идентификационных данных к переносному устройству связи от централизованного компьютера;

- предоставления, от централизованного компьютера системе авторизации, функционально ассоциированной с точкой электронного управления, динамических временных идентификационных данных, идентификатора торговой точки для вероятных

30 торговых точек, идентификатора пользователя, ассоциированного с переносным устройством связи, и срока истечения для динамических временных идентификационных данных; и

- проверки, в системе авторизации, транзакции с динамическими временными идентификационными данными, которые были приняты от точки электронного

35 управления определенного типа в пределах вероятной торговой точки до срока истечения.

13. Способ по п. 12, дополнительно содержащий операции:

- передачи, от централизованного компьютера переносному устройству связи, идентификатора торговой точки для вероятной торговой точки; и

40 приема, централизованным компьютером, проверки правильности вероятной торговой точки от переносного устройства связи.

14. Способ по п. 12, в котором переносное устройство связи обладает однозначной цифровой подписью, а операция проверки дополнительно содержит проверку ассоциации между конечным пользователем и однозначной цифровой подписью.

45 15. Способ по п. 12, в котором способ дополнительно содержит следующие операции авторизации:

- замену данных платежа по обычной карточке, ассоциированных с конечным пользователем переносного устройства связи для динамических временных

идентификационных данных в записи транзакции, и

- прохождение записи транзакции в систему авторизации эмитента для оплаты, используя данные платежа по обычной карточке, ассоциированные с конечным пользователем.

5

10

15

20

25

30

35

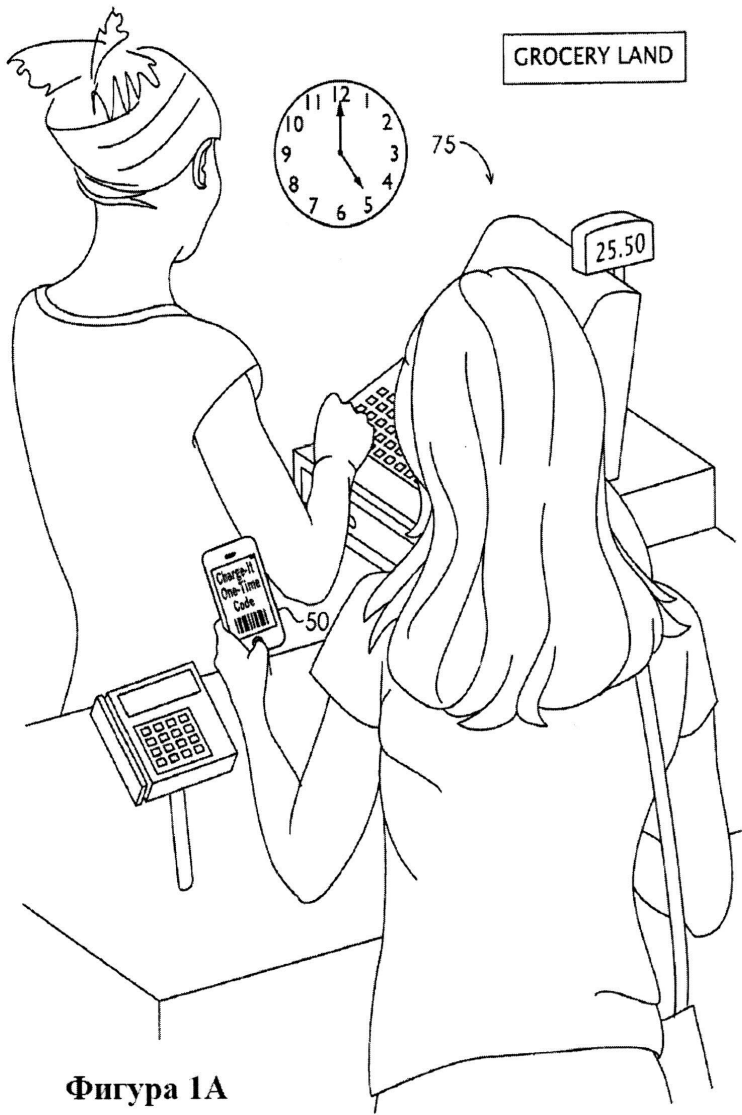
40

45

WO 2013/096486

PCT/US2012/070683

1/11



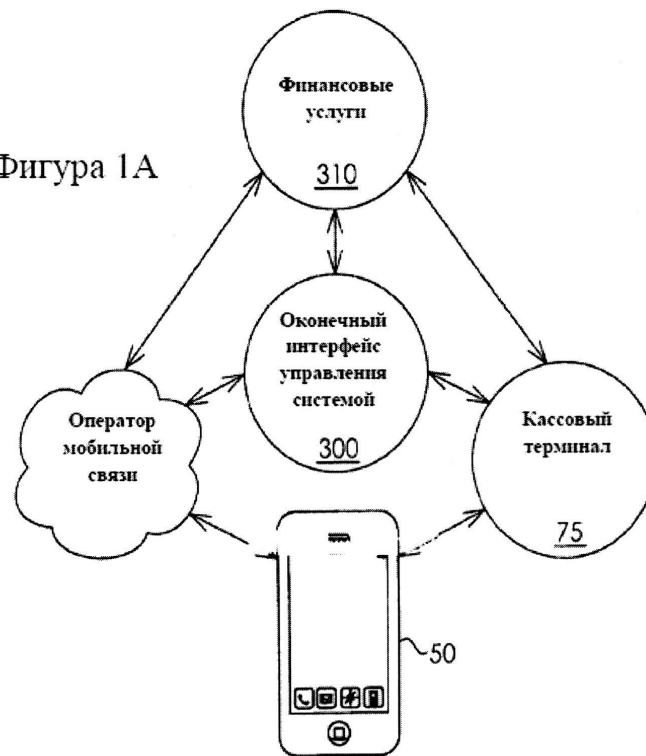
Фигура 1А

WO 2013/096486

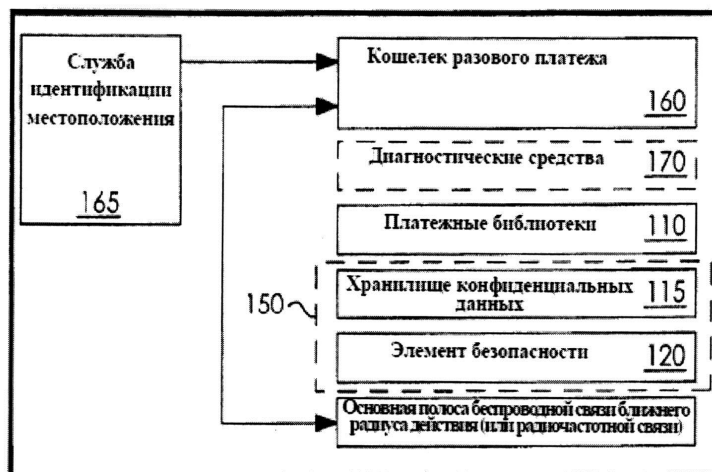
PCT/US2012/070683

2/11

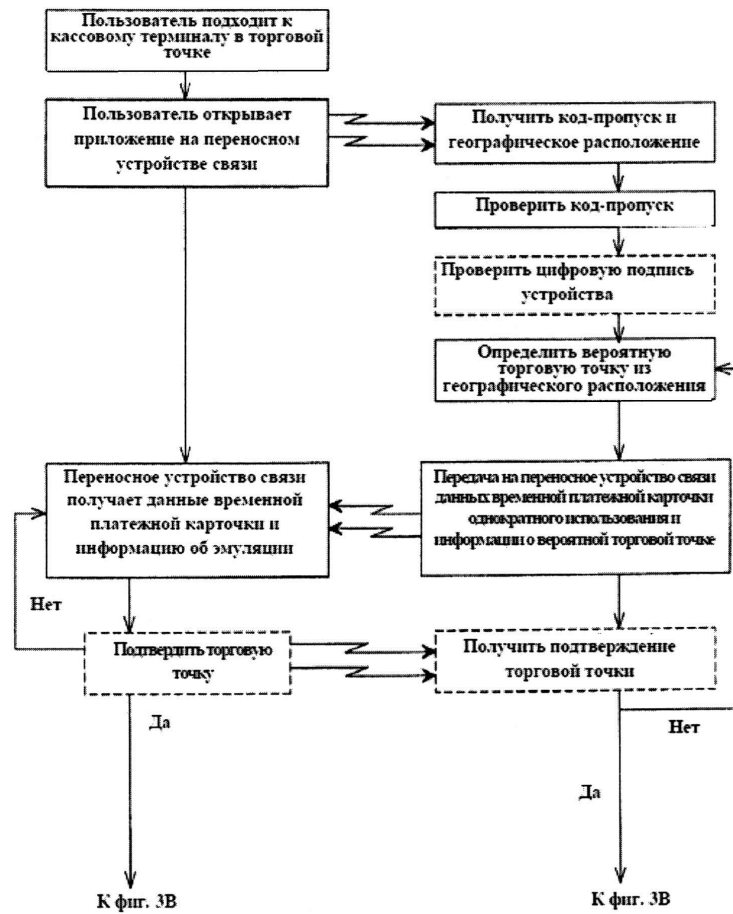
Фигура 1А



Фигура 1В



Фигура 2

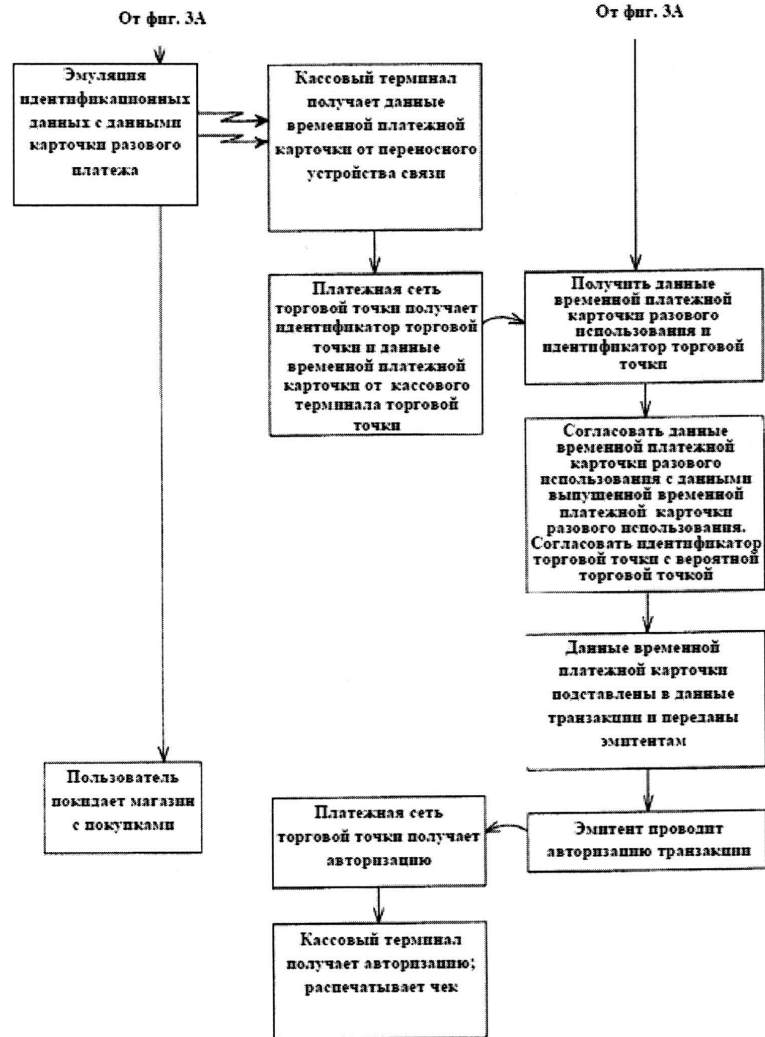


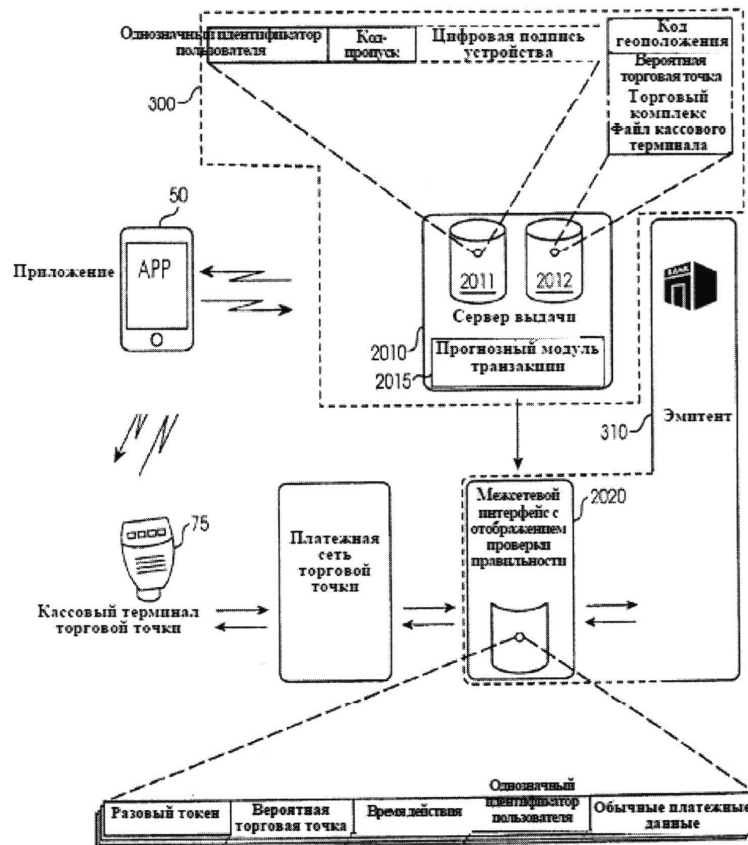
Фигура 3А

WO 2013/096486

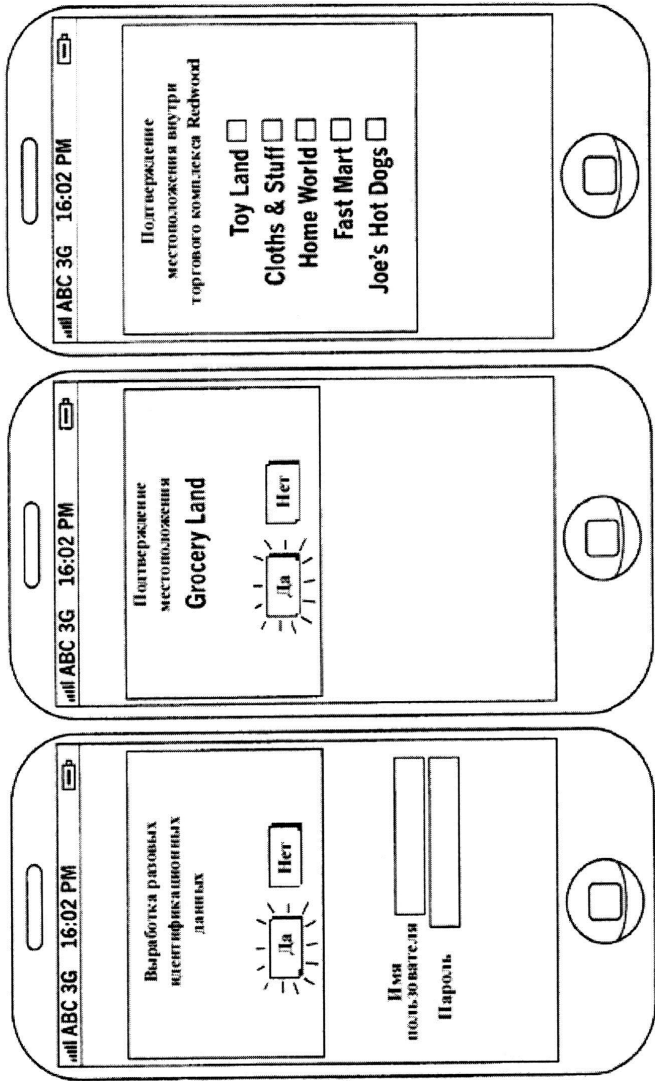
PCT/US2012/070683

5/11





Фигура 4



Фигура 6А

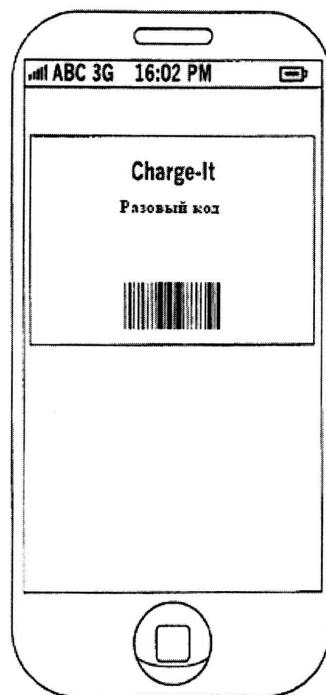
Фигура 6

Фигура 5

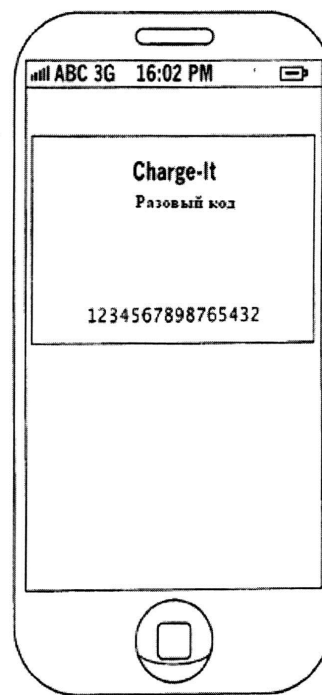
WO 2013/096486

8/11

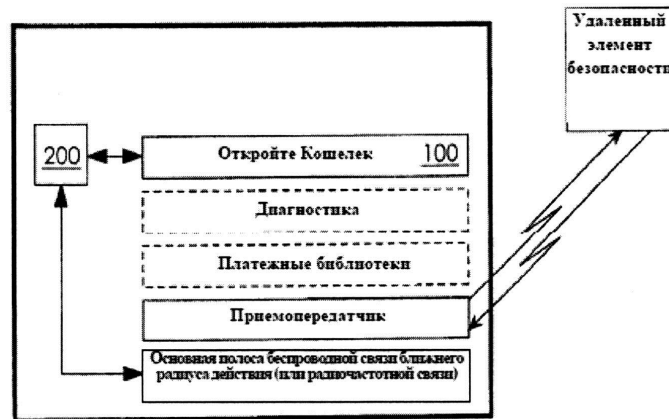
PCT/US2012/070683



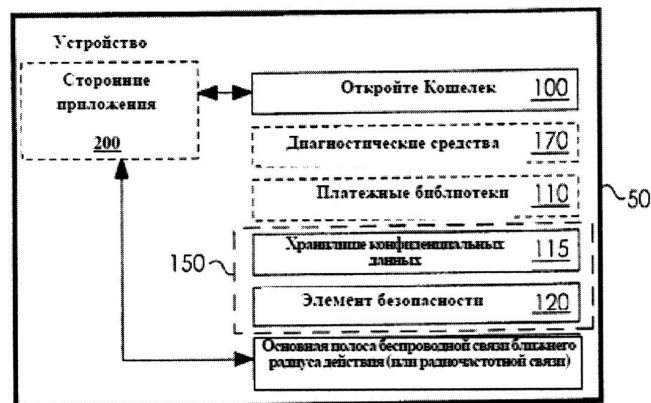
Фигура 7А



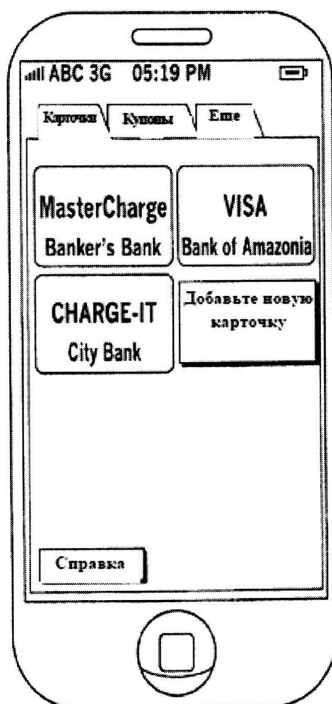
Фигура 7В



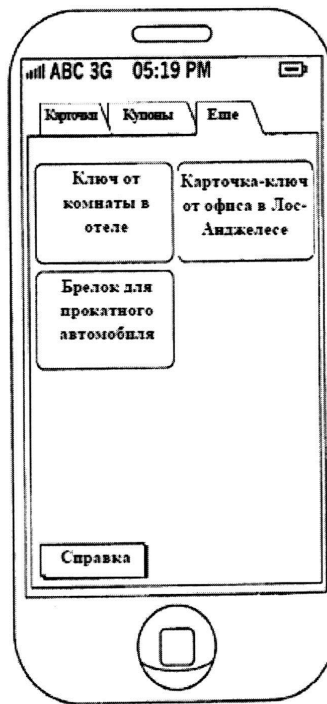
Фигура 8А



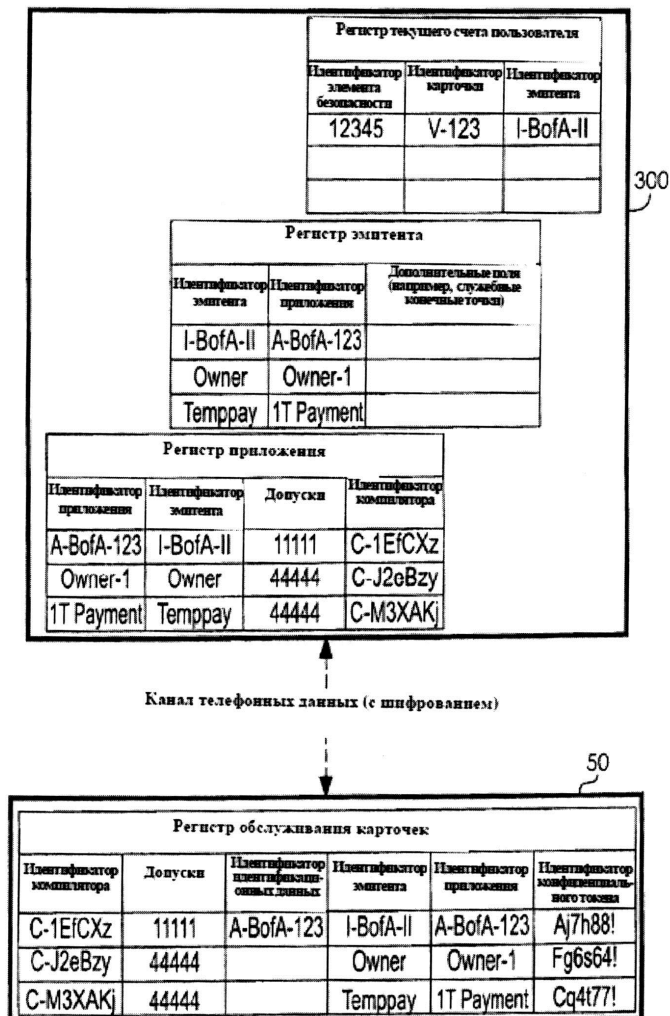
Фигура 8В



Фигура 9А



Фигура 9В



Фигура 10