РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 679 343**(13) **C1**

(51) МПК
G06Q 20/10 (2012.01)
G06Q 20/34 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/20 (2012.01)
G06Q 20/40 (2012.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06Q 20/204 *(2018.08);* ***G06Q 20/3278*** *(2018.08);* ***G06Q 20/341*** *(2018.08);* ***G06Q 20/352*** *(2018.08)*

(21)(22) Заявка: **2017139952, 19.04.2016**

(24) Дата начала отсчета срока действия патента:
19.04.2016

Дата регистрации:
07.02.2019

Приоритет(ы):
(30) Конвенционный приоритет:
20.04.2015 US 14/691,052

(45) Опубликовано: **07.02.2019** Бюл. № **4**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **20.11.2017**

(86) Заявка PCT:
US 2016/028289 (19.04.2016)

(87) Публикация заявки PCT:
WO 2016/172107 (27.10.2016)

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

(72) Автор(ы):
НОЭ Джеймс Кристиан (GB),
ТЬЕРНИ Джон (GB)

(73) Патентообладатель(и):
МАСТЕРКАРД ИНТЕРНЭШНЛ ИНКОРПОРЕЙТЕД (US)

(56) Список документов, цитированных в отчете о поиске: **US 2010/0131413 A1, 27.05.2010. US 2012/0011572 A1, 12.01.2012. US 2013/0262317 A1, 03.10.2013. US 2012/0011070 A1, 12.01.2012. WO 2012/006266 A1, 12.01.2012. RU 2421812 C2, 20.06.2011. RU 2381557 C2, 10.02.2010. RU 2517375 C2, 27.05.2014.**

(54) ВЕРИФИКАЦИЯ БЕСКОНТАКТНОЙ ПЛАТЕЖНОЙ КАРТЫ ДЛЯ ВЫДАЧИ ПЛАТЕЖНОГО УДОСТОВЕРЕНИЯ МОБИЛЬНОМУ УСТРОЙСТВУ

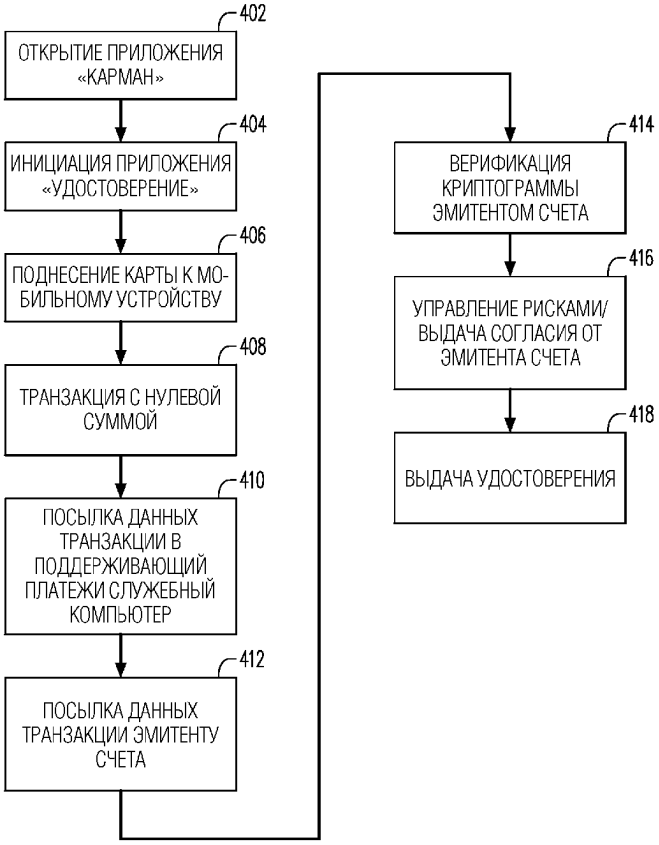
(57) Реферат:

Изобретение относится к способам и мобильному устройству аутентификации бесконтактного платежного устройства с интегральной схемой (IC). Технический результат заключается в обеспечении аутентификации бесконтактного платежного устройства. В способе устанавливают канал связи с мобильным устройством, принимают криптограмму от мобильного устройства, причем криптограмма переправляется мобильным устройством от бесконтактного IC платежного устройства, которое взаимодействует с мобильным устройством, в ответ на прием и валидацию криптограммы аутентифицируют бесконтактное платежное устройство с IC и в ответ на аутентификацию бесконтактного платежного устройства с IC выдают платежное удостоверение мобильному устройству, причем платежное удостоверение связано с платежным счетом, принадлежащим пользователю мобильного устройства, и включает в себя номер основного счета (PAN) или платежный токен, при этом выдача платежного удостоверения содержит этап, на котором сохраняют PAN или платежный токен, соответственно, в элементе безопасности в мобильном устройстве или в защищенном

RU 2679343 C1

RU 2679343 C1

удаленном хост-сервере. 3 н. и 10 з.п. ф-лы, 5 ил.



ФИГ. 4

RU 2679343 C1

RU 2679343 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 679 343**(13) **C1**

(51) Int. Cl.
G06Q 20/10 (2012.01)
G06Q 20/34 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/20 (2012.01)
G06Q 20/40 (2012.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06Q 20/204 (2018.08); G06Q 20/3278 (2018.08); G06Q 20/341 (2018.08); G06Q 20/352 (2018.08)

(21)(22) Application: **2017139952, 19.04.2016**

(24) Effective date for property rights:
19.04.2016

Registration date:
07.02.2019

Priority:
(30) Convention priority:
20.04.2015 US 14/691,052

(45) Date of publication: **07.02.2019** Bull. № **4**

(85) Commencement of national phase: **20.11.2017**

(86) PCT application:
US 2016/028289 (19.04.2016)

(87) PCT publication:
WO 2016/172107 (27.10.2016)

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

(72) Inventor(s):
NOE James Christian (GB),
TIERNEY John (GB)

(73) Proprietor(s):
MASTERCARD INTERNATIONAL INCORPORATED (US)

RU 2679343 C1

(54) VERIFICATION OF CONTACTLESS PAYMENT CARD FOR ISSUING PAYMENT CERTIFICATE FOR MOBILE DEVICE

(57) Abstract:

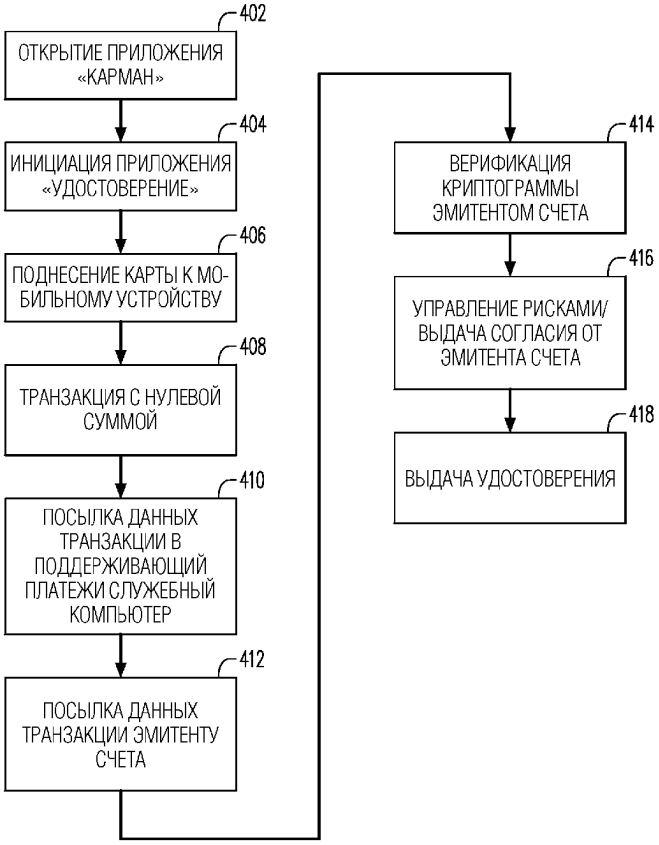
FIELD: cryptography.

SUBSTANCE: invention relates to methods and a mobile device for authentication of a contactless payment device with an integrated circuit (IC). In the method, a communication channel with a mobile device is established, a cryptogram from the mobile device is received, the cryptogram is forwarded by the mobile device from the contactless IC payment device, which communicates with the mobile device, in response to receiving and validating the cryptogram, the contactless payment device with IC is authenticated and, in response to authentication of the contactless payment device with IC, a payment certificate is issued to the mobile device, the payment certificate is associated with the payment account owned by the user of the mobile device, and includes the primary account number (PAN) or payment token, the issuance of the payment certificate contains the stage at which the PAN or payment token is stored, respectively, in the security element in the mobile device or in a secure remote host server.

EFFECT: providing authentication of a contactless payment device.

13 cl, 5 dwg

RU 2679343 C1



ФИГ. 4

RU 2679343 C1

УРОВЕНЬ ТЕХНИКИ

Платежные счета широко используются. В пункте продажи такие счета могут использоваться для покупочных транзакций и могут быть доступны устройствам, таким как карты с магнитной полосой, бесконтактные или контактные карты с микросхемой (IC), иногда именуемые "смарт-картами", или EMV карты (карты, работающие в соответствии с хорошо известным EMV стандартом), или способным к платежам мобильным устройствам, таким как способные к платежам смартфоны, умные часы, браслеты, бирки/этикетки, и т.п. В случае способного к платежам мобильного устройства оно может имитировать бесконтактную платежную карту вхождением в двустороннюю связь с терминалом пункта продажи (POS).

В некоторых мобильных реализациях используется способ, называемый "токенизацией". Это подход, в котором платежное удостоверение (такое как номер основного счета - PAN) запоминается на устройстве и четко отличается от платежного удостоверения, видимого держателю счета. Сервис-провайдер, являющийся третьей стороной, может действовать в качестве "хранилища токенов" с ответственностью за генерацию данных токена, отображение данных токена в исходные (например, PAN) данные и любые криптографические функции, относящиеся к данным токена. Токены выполняются с возможностью выглядеть и действовать подобно обычным картам, когда представляются терминалам. (Различные аспекты и случаи использования, относящиеся к практическому применению токенизации, описаны в "Стандарте совместимости платежных токенов" ("Стандарте токенизации"), опубликованном в ноябре 2013 г. MasterCard International Incorporated (которая является правообладателем этого), Visa и American Express).

Связь с обменом данными) в пункте продажи, с использованием мобильного устройства в качестве реализации платежного устройства, может включать в себя передачу индикатора платежного счета - PAN (номера основного счета) или платежного токена - от способного к платежам мобильного устройства к POS терминалу. POS терминал может затем генерировать сообщение с запросом на авторизацию транзакции, включающее в себя индикатор платежного счета, и это сообщение с запросом на авторизацию транзакции может затем быть направлено (с детокенизацией, если необходимо) эмитенту платежного счета.

В соответствии с процессом, называемым "выдачей", удостоверение платежного счета может быть загружено от центрального компьютера в мобильное устройство, с тем чтобы мобильное устройство могло осуществить упомянутую выше платежную функцию. Согласно некоторым предложениям, выдача может происходить через воздушную линию связи в мобильное устройство. Согласно некоторым предложениям, в качестве части процесса выдачи/установки пользователь может ввести вручную в мобильное устройство PAN, показанный на платежной карте пользователя, который теперь будет имитироваться мобильным устройством. Однако ручной ввод номера счета может быть не очень удобной операцией с точки зрения пользователя, и может быть предрасположен к ошибкам при вводе цифр номера счета. Кроме того, такой подход не гарантирует, что пользователь обладает аутентичной платежной картой, так как пользователь может иметь неправильно полученный мошеннический PAN или может считывать PAN с поддельной платежной карты. А также карты, выпущенные некоторыми эмитентами платежных счетов, могут не иметь PAN или токена, и/или даты истечения срока действия, и/или кода безопасности, напечатанного или нанесенного тиснением на карте, и в этом случае пользователь не будет знать деталей удостоверения.

Согласно другому предложению, камера на мобильном устройстве может быть

использована для захвата изображения PAN на карте, для того чтобы ввести PAN в мобильное устройство. Хотя это может быть быстрее и удобнее, чем ручной, цифра за цифрой, ввод PAN, остается риск для эмитента счета, что изображение захвачено из поддельной карты или из поддельного изображения карты, и не решает проблемы, когда один или более требуемых элементов отсутствуют на карте.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Признаки и преимущества некоторых вариантов осуществления настоящего изобретения, и способ, посредством которого они выполняются, станут более очевидными при рассмотрении последующего описания в сочетании с сопроводительными чертежами, которые иллюстрируют предпочтительные и приводимые в качестве примера варианты осуществления и которые не обязательно выполняются в масштабе.

ФИГ. 1 - блок-схема, представляющая систему для выдачи платежного удостоверения мобильному устройству в соответствии с аспектами настоящего изобретения.

ФИГ. 2 - способное к платежам мобильное устройство, выполненное в соответствии с аспектами настоящего изобретения, которое может быть использовано в связи с системой на фиг. 1.

ФИГ. 3 - блок-схема, представляющая компьютерную систему, которая может работать как часть системы на фиг. 1 и в соответствии с аспектами настоящего изобретения.

ФИГ. 4 - блок-схема последовательности операций, представляющая процесс, который может быть выполнен в системе на фиг. 1, в соответствии с аспектами настоящего изобретения.

ФИГ. 5 - блок-схема последовательности операций, представляющая детали процесса на фиг. 4.

ПОДРОБНОЕ ОПИСАНИЕ

Сегодня некоторые мобильные платежные системы реализуют систему, известную как "токенизация". Такая система работает описанным ниже образом.

- Эмитент платежной карты регистрирует и конфигурирует себя с услугой токенизации. Такие услуги часто предоставляются платежными системами, такими как MasterCard, или могут предоставляться другими подходящими процессорами третьей стороны.

- Конечные пользователи затем регистрируют реквизиты своих платежных карт - это делается ими открытием приложения "кошелек" на устройстве и вводом реквизитов их платежных карт или набором вручную PAN, имени держателя карты, даты истечения срока действия и кода безопасности карты (например, CVC2) (или их сочетания), или же использованием камеры устройства для автоматического захвата и ввода реквизитов.

- Затем реквизиты посылаются от устройства сервис-провайдеру "кошелька" и через него в службу токенизации.

- Служба токенизации проверяет, что реквизиты исходят от карты, которая зарегистрирована для услуги, и если так, то она передает реквизиты эмитенту карты.

- Эмитент карты затем принимает решение, разрешить или нет токенизацию, отклонить токенизацию или потребовать дополнительную аутентификацию пользователя (в этом случае предпринимаются другие шаги для аутентификации пользователя, такие как звонок в call-центр, SMS верификация, мобильная или интернет банковская аутентификация, и т.п.).

- После утверждения и аутентификации служба токенизации генерирует ряд токен удостоверений, которые могут включать в себя номер токен карты, дату истечения

срока действия токена и платежные параметры токена (такие как код валюты, коды стран, код действий эмитента, и т.п.), которые могут быть затем доставлены на телефон (заметим, что возможно также создать токен и загрузить его в телефон, когда происходит аутентификация - токен станет активным, только когда пользователь будет полностью аутентифицирован).

Во время транзакции происходят перечисленные ниже действия.

- **Бесконтактно**

- Пользователь постукивает своим телефоном по бесконтактному терминалу в магазине, чтобы сделать платеж.

- Пользователю может быть предложено аутентифицировать себя устройству (например, используя PIN или биометрически).

- Транзакция отсылается в обслуживающий банк продавца, который, в свою очередь, отсылает ее в платежную систему.

- Если платежная система (или эмитент карты) знает, что транзакция была совершена с токеном, она будет:

- проверять криптографию, если присутствуют EMV данные;

- проверять любые динамические значения (такие как динамический код безопасности) для бесконтактных транзакций с магнитной полосой;

- выполнять другие проверки процессинга, которые требуются;

- переводить реквизиты токена в реальные реквизиты платежной карты;

- производить любые другие изменения элементов данных, специфические для системы;

- посылать транзакцию эмитенту карты.

- Затем эмитент карты будет выполнять свою обычную авторизацию или же может выполнять дополнительные логические функции, когда он знает, что транзакция была совершена с токеном.

-Затем эмитент карты пошлет ответ платежной системе, которая, в свою очередь, выполняет обратный перевод PAN в токен и посылает данные обратно в обслуживающий банк и затем продавцу.

- **Через приложение (in App)**

- Подобно бесконтактному варианту, но транзакции будут инициироваться изнутри приложения продавца.

Один ключевой момент в приведенном выше варианте осуществления по созданию изначального токена заключается в том, что он полностью полагается на пользователя, знающего все (или достаточное число) реквизиты платежной карты. Не все эмитенты карт делают все эти реквизиты доступными для своих клиентов; например, в Нидерландах обычно практически принято не печатать или не тиснить PAN на карте. Без этих реквизитов регистрация карты при современных процессах становится невозможной, и большие группы пользователей будут отстранены от использования таких услуг. Кроме того, ручной ввод реквизитов карты может быть подвержен ошибкам и открыт для мошенничества.

В общем случае и в целях представления концепций вариантов осуществления настоящего изобретения мобильное устройство, такое как смартфон, может быть запрограммировано для эмулирования EMV терминала таким образом, чтобы он мог взаимодействовать с бесконтактной платежной картой, и мобильное устройство также может быть запрограммировано, чтобы быть способным к обеспечению платежного удостоверения в пункте продажи. В процессе облегчения выдачи платежного удостоверения мобильному устройству взаимодействие может происходить между

мобильным устройством и бесконтактной платежной картой, которая должна быть "оцифрована" в мобильное устройство (то есть иметь соответствующее платежное удостоверение, выданное мобильному устройству). В качестве части взаимодействия с мобильным устройством бесконтактная платежная карта может генерировать криптограмму, которую она передает в мобильное устройство. Например, мобильное устройство может быть запрограммировано на эмулирование считывающего терминала бесконтактной карты, и взаимодействие с бесконтактной платежной картой может быть транзакцией с нулевой суммой платежа. Опытные мастера своего дела должны быть знакомы с типами EMV "Прикладных криптограмм", которые могут быть использованы в этом случае (TC, ARQC или AAC), а также они должны быть знакомы с другими использованиями динамических данных, таких как dCVC3, для того чтобы верифицировать определенную карту, которая была использована.

Мобильное устройство может передавать криптограмму, генерируемую (вместе с любыми другими уместными данными, включающими в себя (но не ограничиваясь ими) PAN, дату истечения срока действия, порядковый номер PAN, и т.п.) бесконтактной платежной картой, в служебный компьютер, поддерживающий дистанционные платежи. Это может происходить напрямую или через сервис-провайдера "кошелька", с которым пользователь мобильного устройства зарегистрирован. Служебный компьютер, поддерживающий дистанционные платежи, может передавать криптограмму эмитенту счета, связанному с платежным удостоверением, которое должно быть выдано. Эмитент счета может верифицировать криптограмму и затем согласиться на выдачу платежного удостоверения. Истинное наличие правильной криптограммы указывает с высокой степенью достоверности, что карта была представлена. Служебный компьютер, поддерживающий дистанционные платежи, или подходящая пользующаяся доверием третья сторона, может затем выдать платежное удостоверение мобильному устройству. Альтернативно в некоторых вариантах осуществления безопасное приложение в мобильном устройстве может выполнять аутентификацию карты.

При таком подходе существует высокая степень уверенности, что информация карты/счета, будучи оцифрованной/выданной в мобильное устройство, основана на владении пользователем правильной бесконтактной платежной картой. Более того, автоматическое считывание бесконтактной платежной карты мобильным устройством может сделать процесс выдачи очень удобным для пользователя. Однако наличие только лишь карты может оказаться недостаточным для завершения оцифровывания, и эмитент счета может (по его усмотрению или в соответствии с местными законами, наработанными правилами, или же правилами сервис-провайдера "кошелька") потребовать дополнительной идентификации и верификации (ID&V) покупателя, пытающегося оцифровать карту. Это препятствует оцифровыванию в устройство новой украденной карте.

На фиг. 1 показана блок-схема, которая представляет систему 100, выполненную в соответствии с аспектами настоящего изобретения. Система 100 облегчает выдачу платежного удостоверения мобильному устройству 102. В целях иллюстрации предполагается, что мобильное устройство 102 является способным к платежам смартфоном, но оно может быть любым подходящим устройством, таким как планшетный компьютер, умные часы, персональный компьютер, и т.п. Детали мобильного устройства 102 будут описаны ниже со ссылкой на фиг. 2.

Также на фиг. 1 показана бесконтактная платежная карта 104. В некоторых вариантах осуществления бесконтактная платежная карта может быть полностью традиционной и типа, способного к взаимодействию с POS терминалом без непосредственного

электрического контакта. Таким образом, бесконтактная платежная карта 104 может именоваться как "бесконтактная" платежная карта. Как показано позицией 106 и в соответствии с дополнительным обсуждением ниже, мобильное устройство 102 и бесконтактная платежная карта 104 находятся в беспроводной ближней радиосвязи по передаче данных друг с другом. Бесконтактная платежная карта может быть такой, которая реализует любую или обе возможности из платежей на основе интегральной схемы (такой как MasterCard's M/Chip Advance) или бесконтактных транзакций с магнитной полосой.

Необязательным компонентом системы 100 является сервис-провайдер "кошелька", представленный блоком 108 на фиг. 1. Сервис-провайдер "кошелька", если он присутствует, может поддерживать установку и работу функции цифрового кошелька в мобильном устройстве 102.

Как часть системы 100 показан также поддерживающий платежи служебный компьютер 110. Детали поддерживающего платежи служебного компьютера 110 будут описаны ниже со ссылкой на фиг. 3. Поддерживающий платежи служебный компьютер 110 может обеспечить ряд поддерживающих услуг, чтобы помочь эмитентам платежных счетов в работе с системой платежных счетов. Выдача платежных удостоверений мобильным устройствам по поручению эмитентов счетов может находиться среди услуг, обеспечиваемых поддерживающим платежи служебным компьютером 110. В некоторых вариантах осуществления поддерживающий платежи служебный компьютер 110 может управляться оператором платежной сети. Одна их хорошо известных платежных сетей управляется MasterCard International Incorporated, ее правообладателем. Должно быть понятно, что бесконтактная платежная карта 104 и мобильное устройство 102 (будучи полностью запрограммированными и снабженными) могут быть сконфигурированы для вхождения в транзакции системы платежного счета того типа, которые обрабатываются платежной сетью, такой как управляемая ее правообладателем.

В некоторых вариантах осуществления поддерживающий платежи служебный компьютер 110 может служить в качестве "токен сервис-провайдера", как эта функциональная роль определена в Стандарте токенизации, упомянутом выше. В других вариантах осуществления поддерживающий платежи служебный компьютер 110 может совместно взаимодействовать с токен сервис-провайдером, который не показан отдельно. Как будет обсуждено ниже, в некоторых вариантах осуществления платежное удостоверение, которое должно быть выдано мобильному устройству 102 от поддерживающего платежи служебного компьютера 110, может включать в себя "платежный токен", который заменяет PAN (номер основного счета) в соответствии с положениями Стандарта токенизации. В других вариантах осуществления PAN может быть частью доставленных данных.

Блок 112 на фиг. 1 представляет эмитента платежного счета, который должен быть оцифрован в мобильное устройство 102. Заметим, что блоки 112 и 108 должны оба рассматриваться как представляющие не только указанную организацию, но также одну или более компьютерных систем, управляемых соответствующей организацией или по ее поручению.

Позицией под номером 114 обозначены средства связи, посредством которых мобильное устройство связывается с целью обмена данными с другими компонентами системы 100. Средства 114 связи, например, могут включать в себя участки мобильной сети связи (не показана отдельно), для которой мобильное устройство 102 является абонентским устройством. Кроме того, средства 114 связи могут включать в себя

участки сети Internet или других сетей передачи данных (не показаны отдельно), так что канал передачи данных может быть установлен между мобильным устройством 102 и сервис-провайдером 108 "кошелька" и/или поддерживающим платежи служебным компьютером 110.

Практический вариант осуществления системы 100 может включать в себя многочисленные примеры бесконтактных платежных карт и способных к платежам мобильных устройств, а также, потенциально, значительное число эмитентов счетов. Может быть также и ряд сервис-провайдеров "кошелька" и, возможно, более одного поддерживающего платежи служебного компьютера.

На фиг. 2 показана блок-схема, которая представляет пример варианта осуществления мобильного устройства 102, показанного на фиг. 1 и выполненного в соответствии с аспектами настоящего изобретения. Мобильное устройство 102 может быть традиционным в аспекте своего аппаратного обеспечения. Например, мобильное устройство 102 может быть смартфоном и может быть похожим, в некоторых или во всех аспектах аппаратного обеспечения и во многих своих функциях, на обычные имеющиеся в продаже смартфоны. Альтернативно мобильное устройство 102 может быть планшетным компьютером с возможностями мобильной дистанционной связи. Последующее описание мобильного устройства 102 основано на предположении, что оно реализовано как смартфон; специалисты в данной области техники без труда поймут из последующего описания, как реализовать мобильное устройство 102 в виде планшетного компьютера или другого устройства, отличающегося от смартфона.

Мобильное устройство 102 может включать в себя традиционный корпус (обозначенный пунктирной линией 202 на фиг. 2), который содержит и/или поддерживает другие компоненты мобильного устройства 102. Корпус 202 может иметь такие форму и размеры, чтобы пользователь мог держать его в руке, и может, например, иметь конструктивные параметры, обычные для сегодняшнего поколения смартфонов.

Мобильное устройство 102 дополнительно включает в себя традиционную схему 204 управления для управления всей работой мобильного устройства 102. Например, схема 204 управления может включать в себя обычный процессор, тип которого выполнен с возможностью служить "мозгом" смартфона.

Другие компоненты мобильного устройства 102, которые находятся в связи и/или управляются схемой 204 управления, включают в себя: (a) одно или более запоминающих устройств 206 (например, память программ и оперативная память, и т.п.);(b) обычную SIM (модуль идентификации абонента) карту 208; (c) обычный сенсорный экран 212, который служит в качестве основного устройства ввода/вывода для мобильного устройства 102 и который, таким образом, принимает входную информацию от пользователя и воспроизводит выходную информацию для пользователя. Как и в случае с многими моделями смартфонов, в некоторых вариантах осуществления мобильное устройство 102 может также включать в себя несколько приводимых в действие физически выключателей/органов управления (не показаны), таких как переключатель включения/выключения/перезагрузки, кнопка меню, кнопка "возврат", регулятор громкости, и т.п. Может также существовать случай, когда мобильное устройство 102 включает в себя обычную цифровую камеру, которая не показана.

Мобильное устройство 102 также включает в себя обычную схему 216 приема/передачи, которая также находится в связи и/или управляется схемой 204 управления. Схема 216 приема/передачи соединена с антенной 218 и обеспечивает канал(ы) связи, посредством которых мобильное устройство 102 связывается через мобильную телефонную сеть связи (которая, например, включена в состав вышеупомянутых средств

114 связи на фиг. 1).

Продолжая ссылаться на фиг. 2, схема 216 приема/передачи может работать как для приема, так и для передачи голосовых сигналов в дополнение к выполнению функций передачи данных. Как известно специалистам в данной области техники, такая передача данных может осуществляться через HTTP (протокол передачи гипертекста) или другой коммуникационный протокол, подходящий для выполнения передачи данных через Internet.

Мобильное устройство 102 дополнительно включает в себя обычный микрофон 220, подсоединенный к схеме 216 приема/передачи. Конечно, микрофон 220 служит для приема голоса, поступающего от пользователя. Дополнительно динамик 222 включен в состав для обеспечения выходного звукового сигнала для пользователя, и он подсоединен к схеме 216 приема/передачи.

Схема 216 приема/передачи может работать обычным образом для передачи через антенну 218 голосовых сигналов, генерируемых микрофоном 220, и для воспроизведения через динамик 220 голосовых сигналов, принятых через антенну 218. Схема 216 приема/передачи может также обслуживать передачу и прием текстовых сообщений, и другой обмен данными через антенну 218.

Мобильное устройство 102 может также включать в себя схему 224, которая частично или полностью предназначена для реализации функций NFC связи мобильного устройства 102. Мобильное устройство 102 может дополнительно включать в себя петлевую антенну 226, соединенную с NFC схемой 224. В некоторых вариантах осуществления NFC схема 224 может частично перекрываться со схемой 204 управления для мобильного устройства 102. Кроме того, NFC схема 224 связана, и может также перекрываться, с элементом 228 безопасности, который является частью мобильного устройства 102 и содержится внутри корпуса 202. Термин "элемент безопасности" хорошо известен специалистам в данной области техники и обычно относится к устройству, которое может включать в себя небольшой процессор и энергозависимую и энергонезависимую память (не показаны отдельно), которые защищены от постороннего вмешательства и/или перепрограммирования подходящими мерами. В некоторых вариантах осуществления элемент 228 безопасности может быть обеспечен как часть SIM карты 208. В других вариантах осуществления элемент 228 безопасности может быть образован картой интегральной схемы, отдельной от SIM карты 208, но, возможно, имеющей один и тот же форм-фактор, как и SIM карта 208. В некоторых вариантах осуществления мобильного устройства 102 элемент 228 безопасности может быть традиционным в аспекте аппаратного обеспечения. В некоторых вариантах осуществления функциональные возможности, описанные ниже, могут быть запрограммированы в элемент безопасности и/или процессинговые элементы в мобильном устройстве 102 в соответствии с аспектами настоящего изобретения. (Следует заметить, что термин "элемент безопасности" не ограничен только устройствами на основе интегральных схем (IC), напротив, он может также включать в себя любую обеспечивающую безопасность среду в мобильном устройстве и может включать в себя основанную на программном обеспечении среду, обеспечивающую безопасность, работающую на процессоре мобильного устройства). В некоторых вариантах осуществления элемент 228 безопасности может быть снабжен или перепрограммирован одной или более прикладных платежных программ ("apps"), с тем чтобы мобильное устройство могло работать как платежное устройство напрямую с POS терминалами. С этой целью мобильное устройство 102 может связываться с POS терминалами через антенну 226 в соответствии с NFC стандартом связи. Кроме того, согласно аспектам

настоящего изобретения, элемент 228 безопасности или другой программируемый компонент(ы) мобильного устройства 102 может быть запрограммирован таким образом, что мобильное устройство 102 сможет работать как считывающее устройство или терминал по отношению к бесконтактной платежной карте. С этой целью одно или более платежных приложений могут быть подходящим образом дополнены соответствующими программными командами, или же отдельное приложение может быть установлено в мобильное устройство 102, чтобы обеспечить функциональные возможности считывающего устройства/терминала. В случае либо дополненного платежного приложения, либо специализированного приложения считывающего устройства/терминала антенна 226 может быть использована приложением для вхождения в NFC связь с бесконтактной платежной картой в соответствии с описанными здесь процессами.

Чтобы подытожить и дополнить кое-что из вышесказанного, мобильное устройство 102 может иметь одно или более из: (i) встроенного элемента безопасности; (ii) элемента безопасности, основанного на SIM карте; (iii) другой формы безопасно запоминающих приложений и удостоверений, таких как SD карта; (iv) поддержки облачных платежей (например, для функциональной возможности, называемой "HCE" в среде Android; или, как предложено в связи с инициативой MasterCard Cloud Based Payments, выдвинутой ее правообладателем); (v) доверенной среды выполнения (TEE) для выполнения относящихся к платежам приложений. Дополнительно или альтернативно другие связанные с безопасностью признаки могут быть использованы на мобильном устройстве 102 в этом отношении, включая сюда связанные с безопасностью признаки, представленные ниже.

Должно быть понятно, что мобильное устройство 102 может управляться как обычный мобильный телефон для связи - как голосовой, так и для передачи данных - по обычной мобильной телекоммуникационной сети, которая не изображена на чертеже независимо от элемента 114 на фиг. 1. Так что мобильное устройство 102 может время от времени связываться обычным образом с оператором мобильной сети ("MNO" - не показан).

Как известно специалистам в данной области техники, мобильное устройство 102 может рассматриваться как малое компьютерное устройство. Мобильное устройство 102 может включать в себя один или более процессоров, которые программируются программным обеспечением, приложениями и/или другими выполняемыми процессором этапами для обеспечения функциональных возможностей, описанных здесь. Программное обеспечение, приложения и/или другие выполняемые процессором этапы могут запоминаться в одном или более машиночитаемых носителях данных (таких как запоминающие устройства 206 и/или элемент 208 безопасности) и могут содержать программные команды, которые могут именоваться машиночитаемыми средствами программного кода.

На фиг. 3 показана блок-схема, которая представляет приводимый в качестве примера вариант осуществления поддерживающего платежи служебного компьютера 110, показанного на фиг. 1.

Поддерживающий платежи служебный компьютер 110 может быть образован стандартными компонентами в контексте его аппаратного обеспечения и архитектуры, но может управляться программным обеспечением, чтобы заставить его функционировать, как описано здесь. Например, поддерживающий платежи служебный компьютер 110 может быть образован аппаратными средствами сервер-компьютера.

Поддерживающий платежи служебный компьютер 110 может включать в себя

процессор 300 компьютера, функционально связанный с коммуникационным устройством 301, запоминающее устройство 304, входное устройство 306 и выходное устройство 308.

Процессор 300 компьютера может быть образован одним или более процессорами. Процессор 300 работает для выполнения выполняемых процессором этапов, содержащихся в программных командах, описанных ниже, с тем чтобы осуществлять управление поддерживающим продажи служебным компьютером 110 для обеспечения описанных функциональных возможностей.

Коммуникационное устройство 301 может быть использовано для облегчения связи, например, с другими устройствами (такими как компьютер или компьютеры, управляемые сервис-провайдером или провайдерами "кошелька" и/или эмитентами счетов, и/или мобильные устройства, такие как мобильное устройство 102, показанное на фиг. 1). Например, (и продолжая ссылаться на фиг. 3) коммуникационное устройство 301 может содержать многочисленные коммуникационные порты (отдельно не показаны), чтобы позволить поддерживающему платежи служебному компьютеру 110 связываться одновременно с рядом других компьютеров и другими устройствами.

Входное устройство 306 может содержать одно или более периферийных устройств любого типа, обычно используемых для ввода данных в компьютер. Например, входное устройство 306 может включать в себя клавиатуру и мышь. Выходное устройство 308 может содержать, например, дисплей и/или принтер.

Запоминающее устройство 304 может содержать любое подходящее устройство для запоминания информации, включая сюда сочетание магнитных запоминающих устройств (например, накопители на жестких дисках), оптических запоминающих устройств, таких как CD и/или DVD, и/или полупроводниковых запоминающих устройств, таких как оперативные запоминающие устройства (RAM) и постоянные запоминающие устройства (ROM), а также так называемую флэш-память. Любое одно или более из таких устройств для запоминания информации может рассматриваться как машиночитаемая среда хранения или же машиночитаемый носитель данных или память.

Запоминающее устройство 304 запоминает одну или более программ для управления процессором 300. Программы содержат программные команды (которые могут именоваться машиночитаемыми средствами программного кода), которые содержат выполняемые процессором этапы процесса для поддерживающего платежи служебного компьютера 110, выполняемые процессором 300, чтобы заставить поддерживающий платежи служебный компьютер 110 функционировать, как описано здесь.

Программы могут включать в себя одну или более традиционных операционных систем (не показаны), которые управляют процессором 300, с тем чтобы управлять и координировать действия и совместное использование ресурсов в поддерживающем платежи служебном компьютере 110 и служить в качестве хост-системы для прикладных программ (будут описаны ниже), которые прогоняются на поддерживающем платежи служебном компьютере 110.

Запоминающее устройство 304 может запоминать выдающую удостоверение прикладную программу 310, которая управляет процессором 300, чтобы позволить поддерживающему платежи служебному компьютеру 110 обеспечивать услуги выдачи, посредством которых платежный счет может быть оцифрован в способное к платежам мобильное устройство, в соответствии с аспектами настоящего изобретения.

Продолжая ссылаться на фиг. 3, программы, запомненные в запоминающем устройстве 304, могут также включать в себя прикладную программу 312 для обработки транзакций, которая управляет процессором 300, чтобы позволить поддерживающему

платежи служебному компьютеру 110 обрабатывать запросы на платежные транзакции описанным здесь образом.

Запоминающее устройство 304 может также запоминать, а поддерживающий платежи служебный компьютер 110 может также выполнять другие программы, которые не показаны. Например, такие программы могут включать в себя приложение для создания отчетов, которое может отвечать на запросы от администратора системы для отчетов по действиям, выполненным поддерживающим платежи служебным компьютером 110. Другие программы могут также включать в себя, например, одну или более программ передачи данных, программы управления базой данных, драйверы устройств, и т.п.

Запоминающее устройство 304 может также запоминать одну или более баз 314 данных, требуемых для работы поддерживающего платежи служебного компьютера 110.

Компьютер эмитента счета, представленный блоком 112 на фиг. 1, может быть подобен в аспекте своего аппаратного обеспечения и/или архитектуры аппаратному обеспечению компьютера, описанному выше в связи с фиг. 3. Однако компьютер 112 эмитента счета может иметь другие функции, чем поддерживающий платежи служебный компьютер 110, и, соответственно, может использовать другие программы, отличающиеся от используемых поддерживающим платежи служебным компьютером 110.

На фиг. 4 показана блок-схема последовательности операций, иллюстрирующая процесс, который может выполняться в системе, представленной на фиг. 1.

На этапе 402 пользователь (не показан) может привести в действие мобильное устройство 102, чтобы открыть прикладную программу "кошелек" ("wallet app" - приложение "кошелек") на мобильном устройстве 102. По меньшей мере в некоторых вариантах осуществления это может включать в себя то, что приложение "кошелек" потребует, чтобы процедура аутентификации пользователя была успешно выполнена пользователем. Возможные типы аутентификации пользователя могут включать в себя биометрическую аутентификацию (например, считывание отпечатков пальцев пользователя) или ввод PIN, требуемый для доступа к приложению "кошелек".

Исходя из предположения, что аутентификация пользователя (если она потребовалась) была успешно завершена, затем, по запросу пользователя, приложение "кошелек" может (как указано этапом 404) инициировать операцию для выдачи платежного удостоверения мобильному устройству 102. Обработка на этапе 404 может включать в себя установление канала связи между мобильным устройством 102 и поддерживающим платежи служебным компьютером 110. В некоторых вариантах осуществления этот канал связи может быть образован прокладыванием связи между мобильным устройством 102 и поддерживающим платежи служебным компьютером 110 через сервис-провайдера 108 "кошелька" (если он присутствует). В некоторых вариантах осуществления открытие приложения "кошелек" на этапе 402 может заставить мобильное устройство 102 вступить в контакт с сервис-провайдером "кошелька". Дополнительно или альтернативно обмен данными может происходить непосредственно между мобильным устройством 102 и поддерживающим платежи служебным компьютером 110. (Когда говорится, что данные должны передаваться или приниматься поддерживающим платежи служебным компьютером 110 в мобильное устройство 102 или от него, это включает в себя прямую или опосредствованную передачу данных).

На этапе 406 на фиг. 4 пользователь может поднести бесконтактную платежную карту 104 близко к мобильному устройству 102. Пользователь может сделать это в ответ на подсказку, появившуюся на сенсорном экране 212 мобильного устройства

102. Это может происходить таким образом, что бесконтактная платежная карта 104 и мобильное устройство 102 получают разрешение на вхождение в ближнюю радиосвязь друг с другом. Например, пользователю может быть подсказано, чтобы он постучал бесконтактной платежной картой по мобильному устройству 102 в том месте на мобильном устройстве 102, которое находится рядом с NFC антенной 226 (фиг. 2). Мобильное устройство 102, действующее как считывающее устройство или терминал операции, может передавать запросный сигнал, на который бесконтактная платежная карта 104 может ответить, тем самым подтверждая в результате вхождение в обмен данными между мобильным устройством 102 и бесконтактной платежной картой 104.

На этапе 408, согласно некоторым вариантам осуществления, мобильное устройство 102 и бесконтактная платежная карта 104 могут взаимодействовать друг с другом таким образом, что платежная операция с "нулевой суммой" выполняется двумя этими устройствами. Эта транзакция не обязательно должна быть с нулевой суммой, но если такая транзакция используется, опытные специалисты, знакомые с принципами EMV, поймут, что транзакция с нулевой суммой с меньшей вероятностью приводит к неудаче и с большей вероятностью приводит к успеху - однако принципиально сумма может быть любой величины. Такая транзакция, как понятно для специалистов в данной области техники, может осуществлять обмен данными по электронной почте между бесконтактной платежной картой 104 и мобильным устройством 102. На фиг. 5 показана блок-схема последовательности операций, которая иллюстрирует аспекты транзакции с нулевой суммой, представленной этапом 408.

На фиг. 5 на этапе 502 транзакция может быть запущена, например, подходящей командой или сообщением от мобильного устройства 102 (работающего в качестве считывающего устройства или терминала) в бесконтактную платежную карту 104. На этапе 504 бесконтактная платежная карта 104 может передавать данные счета. На этапе 505 бесконтактная платежная карта 104 и мобильное устройство 102 могут вступать в диалог/обмен сообщениями для установления деталей, касающихся криптограммы, которая должна быть сгенерирована. На этапе 506 бесконтактная платежная карта 104 может вступать в EMV транзакцию или ей подобную с мобильным устройством 102, так что бесконтактная платежная карта 104 может генерировать криптограмму и передавать ее в мобильное устройство 102. Другие типы относящихся к транзакциям процессов могут альтернативно выполняться для криптографической аутентификации бесконтактной платежной карты 104.

Например, в некоторых вариантах осуществления транзакция с нулевой суммой может быть выполнена в соответствии с хорошо известным EMV стандартом для транзакций платежного счета в пункте продажи. В таком случае бесконтактная платежная карта 104 может генерировать и передавать тип криптограммы, обычно требуемый от платежного устройства в EMV транзакции. В других вариантах осуществления транзакция может выполняться в соответствии с практикой, в которой бесконтактная платежная карта 104 имитирует стиль транзакций с "магнитной полосой". В этом последнем типе варианта осуществления бесконтактная платежная карта 104 может генерировать динамический код безопасности (например, тип кода, известный как "dCVC3" или подобный тип кода безопасности). Как известно специалистам в данной области техники, при генерации динамического кода безопасности бесконтактная платежная карта 104 может выполнять криптографический процесс для получения результата, который затем усекается до трех или четырех цифр, и этот усеченный результат служит в качестве динамического кода безопасности. Термин "криптограмма" должен пониматься как включающий в себя такой криптографически генерируемый

динамический код безопасности.

В некоторых вариантах осуществления транзакция не обязательно должна быть с нулевой суммой.

В транзакции с нулевой суммой, представленной этапом 408, бесконтактная платежная карта 104 может также передавать в мобильное устройство 102 данные платежного удостоверения, которые были запомнены в бесконтактной платежной карте 104. Такие данные платежного удостоверения могут включать в себя PAN или платежный токен, связанный с платежным счетом, который должен быть оцифрован в мобильное устройство 102. Данные платежного удостоверения могут также включать в себя другие данные, такие как дата окончания срока действия для рассматриваемого платежного счета. Во многих случаях данные платежного удостоверения будут включать в себя скорее PAN, чем платежный токен. Должно быть также понятно, что, как часть транзакции с нулевой суммой (и как представлено на этапе 508 на фиг. 5), мобильное устройство 102 может принимать криптограмму, генерируемую и передаваемую бесконтактной платежной картой 104, и может также принимать данные платежного удостоверения, передаваемые бесконтактной платежной картой 104, и при этом должно обрабатывать их безопасно.

В некоторых вариантах осуществления взаимодействие между бесконтактной платежной картой 104 и мобильным устройством 102 может отличаться от транзакции с нулевой суммой или другой транзакции в стиле пункта продажи. Например, не следуя стандартному процессу транзакции платежного счета, бесконтактная платежная карта 104 может генерировать криптограмму в соответствии с заданным процессом. Бесконтактная платежная карта может передавать криптограмму и PAN (или другой индикатор счета) мобильному устройству путем обмена данными, который не имитирует транзакцию платежного счета.

Используемый здесь и в формуле изобретения термин "криптограмма" следует понимать как включающий в себя любой результат или итог криптографического процесса, включая сюда усеченные или измененные результаты такого процесса.

Обращаясь снова к фиг. 4, на этапе 410 мобильное устройство 102 может передавать поддерживающему платежи служебному компьютеру - непосредственно или опосредствованно - некоторые или все данные, принятые мобильным устройством 102 от бесконтактной платежной карты 104 как часть транзакции с нулевой суммой на этапе 408. Данные, переданные на этапе 410 мобильным устройством 102, могут включать в себя вышеупомянутую криптограмму/динамический код безопасности и PAN (или другой индикатор счета), принятый мобильным устройством 102 от бесконтактной платежной карты 104. В некоторых вариантах осуществления данные, переданные от мобильного устройства 102, могут быть сформатированы как сообщение авторизации транзакции платежного счета. В некоторых вариантах осуществления данные, переданные от мобильного устройства 102, могут включать в себя данные, которые однозначно идентифицируют мобильное устройство 102. Принимая во внимание канал прямой или опосредствованной передачи данных, устанавливаемый между мобильным устройством 102 и поддерживающим платежи служебным компьютером 110, поддерживающий платежи служебный компьютер 110 может принимать данные, переданные мобильным устройством 102 на этапе 410.

На этапе 412 поддерживающий платежи служебный компьютер 110 может передавать по меньшей мере некоторые из данных транзакции эмитенту 112 счета с указанием, что поддерживающий платежи служебный компьютер 110 запрашивает разрешение от эмитента 112 счета на выдачу платежного удостоверения мобильному устройству 102

по отношению к платежному счету, представленному данными транзакции. (Должно быть понятно, что поддерживающий платежи служебный компьютер 110 может идентифицировать, с каким эмитентом счета устанавливается контакт, основываясь на индикаторе счета, который он принял от мобильного устройства 102). Данные транзакции, переданные поддерживающим платежи служебным компьютером 110 на этапе 412, могут включать в себя, например, криптограмму, генерируемую бесконтактной платежной картой 104, и PAN или другой индикатор счета, считываемый мобильным устройством 102 из бесконтактной платежной карты 104 на этапе 408. Должно быть понятно, что эмитент 112 счета может принимать данные, передаваемые ему поддерживающим платежи служебным компьютером 110 на этапе 412.

На этапе 414 эмитент 112 счета может верифицировать криптограмму, которую он принял от поддерживающего платежи служебного компьютера 110. Например, эмитент счета может выполнять обычный процесс, посредством которого криптограммы или динамические коды безопасности (как возможный случай) верифицируются эмитентами счета в связи с транзакциями платежного счета. Эмитент 112 счета может верифицировать другую информацию, принятую от поддерживающего платежи служебного компьютера 110, такую как достоверность PAN или индикатора счета, принятого от поддерживающего платежи служебного компьютера 110. Эмитент счета может также верифицировать, что рассматриваемый платежный счет находится в хорошем состоянии.

На этапе 416 эмитент 112 счета может вступит в процесс управления/оценки риска по отношению к запросу на выдачу, принятому от поддерживающего платежи служебного компьютера 110. В некоторых вариантах осуществления и/или в некоторых случаях эмитент 112 счета может просто согласиться с запросом (например, в ответ на верификацию криптограммы) и может послать с этой целью сообщение поддерживающему платежи служебному компьютеру 110. В других вариантах осуществления или случаях, например, в результате итога процесса управления риском, эмитент 112 счета может определить, что ID&V (идентификации и верификации) процесс должен быть выполнен. Затем эмитент 112 счета может выполнить ID&V процесс (способом, который знаком специалистам в данной области техники), и исходя из предположения, что процесс имеет положительный результат, эмитент 112 счета может затем согласиться с запросом на выдачу. В некоторых случаях, например, когда ID&V процесс является неудачным, эмитент 112 аккаунта может не дать согласия на запрос о выдаче. В таком случае выдача не может происходить.

Дополнительно или альтернативно к операции выдачи, зависящей от успешной аутентификации бесконтактной платежной карты при посредстве канала через мобильное устройство, система может предпринять другое действие, которое отражает успешную аутентификацию бесконтактной платежной карты. Например, процесс, подобный показанному на фиг. 4, может быть использован как часть двухфакторной схемы безопасности в связи с покупочной транзакцией в электронной торговле.

Например, выше была сделана ссылка на транзакции "через приложение" ("in app"), инициируемые изнутри приложения электронной торговли продавца. Для такой транзакции мобильное устройство покупателя может быть соответственно запрограммировано для взаимодействия с сервер-компьютером электронной торговли продавца, чтобы помочь аутентификации покупателя и подтвердить, что покупатель владеет правильной платежной картой. Таким образом, процесс аутентификации карты может быть выполнен, как описано здесь, с мобильным телефоном покупателя, запрограммированным и оборудованным для взаимодействия с платежной картой

покупателя с целью извлечения криптограммы из платежной карты и передачи криптограммы в приложение электронной торговли продавца для переправления ее эмитенту карты с целью проверки правильности криптограммы. При успешном выполнении этих аспектов безопасности транзакция электронной торговли может продолжаться с высокой степенью уверенности, что покупатель владеет достоверной платежной картой, которая соответствует платежной информации, используемой для транзакции электронной торговли.

Если предположить, что эмитент 112 счета согласился с запросом на выдачу от поддерживающего платежи служебного компьютера 110, то затем этап 418 может следовать за этапом 416. На этапе 418 поддерживающий платежи служебный компьютер 110 может выдать платежное удостоверение мобильному устройству 102. В некоторых вариантах осуществления выдача может происходить подобным образом, как если бы информация о счете была получена ручным вводом информации о счете или фотографическим считыванием информации о счете в мобильном устройстве 102. Платежное удостоверение, выданное мобильному устройству 102, может быть таким же или отличаться от платежного удостоверения, реализованного в платежной карте 104, хотя, как правило, будет так, что платежное удостоверение, выданное мобильному устройству 102, обеспечивает доступ к тому же платежному счету, который доступен через платежную карту 104. Платежное удостоверение, выданное мобильному устройству 102, может в некоторых случаях включать в себя PAN, а в других случаях может включать в себя "платежный токен", как этот термин используется в стандарте токенизации. Платежное удостоверение, выданное мобильному устройству 102, может включать в себя некоторую или всю другую информацию (например, дату истечения срока действия счета и/или токена, имя держателя счета, криптографический ключ, и т.п.), обычно загружаемую в платежную карту во время персонализации карты.

Должно быть понятно, что, не принимая во внимание промежуточные этапы, выдача платежного удостоверения от поддерживающего платежи служебного компьютера 110 мобильному устройству 102 происходит в ответ на прием поддерживающим платежи служебным компьютером криптограммы и/или данных счета от мобильного устройства 102.

Можно сказать, что платежное удостоверение, выданное мобильному устройству на этапе 418, может "согласовываться" с удостоверением, запомненным в бесконтактной платежной карте, в том смысле, что оба ряда удостоверений обеспечивают доступ к одному и тому же платежному счету, принадлежащему пользователю бесконтактной платежной карты 104 и мобильного телефона 102. В одном примере, который находится среди ряда разных возможностей, бесконтактная платежная карта 104 может хранить PAN для платежного счета, тогда как удостоверение, выданное мобильному устройству 102, включает в себя платежный токен, который подменяет этот PAN. Должно быть понятно, что в некоторых вариантах использования удостоверение, выданное мобильному устройству, может включать в себя тот же PAN, что и запомненный в бесконтактной платежной карте.

В некоторых вариантах осуществления выдача платежного удостоверения может включать в себя запоминание PAN или платежного токена и соответствующих данных в элементе 228 безопасности (фиг. 2) в мобильном устройстве 102. В других вариантах осуществления (например, где мобильное устройство не включает в себя основанного на аппаратном обеспечении элемента безопасности) выдача платежного удостоверения может включать в себя запоминание PAN или платежного токена и соответствующих данных в защищенном удаленном хост-сервере (не показан), который обеспечивает

дистанционное эмулирование элемента безопасности. В таких случаях данные, доставленные в защищенный удаленный хост-сервер, могут быть доступны для защищенной от постороннего доступа среды выполнения на мобильном устройстве, как требуется для мобильного устройства для вхождения в транзакцию платежного счета в пункте продажи. В общем случае этап выдачи может включать в себя некоторые или все типы признаков безопасности мобильного устройства, которые описаны выше в связи с фиг. 2.

Процесс на фиг. 4 может быть выигрышным в том отношении, что он предлагает высокую степень удобства пользователю вместе с уменьшением возможности ошибок в доставке информации о счете поддерживающему платежи служебному компьютеру. Кроме того, поскольку процесс включает в себя генерацию криптограммы бесконтактной платежной картой с верификацией криптограммы эмитентом счета, безопасность процесса выдачи повышается. В частности, существует высокая степень вероятности при этом процессе, что пользователь, который инициирует оцифровывание платежного счета, владеет правильной бесконтактной платежной картой, которая представляет счет.

Кроме того, процесс на фиг. 4 позволяет производить оцифровывание платежного счета, даже когда бесконтактная платежная карта пользователя утрачивает видимое представление номера счета.

В вариантах осуществления, которые были описаны выше, бесконтактная платежная карта (то есть имеющий форму карты объект) была использована для предоставления криптограммы (и данных счета) мобильному устройству. Однако альтернативно платежное устройство, которое не имеет форму карты, может быть использовано вместо бесконтактной платежной карты. В этой роли могут быть использованы примеры других типов платежных устройств, включающих в себя браслеты, часы, брелоки, и т.п. Должно быть также понятно, что термин "платежное устройство" включает в себя бесконтактные платежные карты.

Технические приемы, описанные выше применительно к аутентификации платежного устройства, могут быть выигрышными для использования в связи с любым типом процедуры, которая требует или получает выгоду от дистанционного считывания платежного устройства.

Используемы здесь и в прилагаемой формуле изобретения термин "индикатор счета" должен пониматься как включающий в себя как PAN, так и платежные токены.

Используемы здесь и в прилагаемой формуле изобретения термин "компьютер" должен пониматься как применимый к единственному компьютеру, так и к двум или более компьютерам в сочетании друг с другом.

Используемы здесь и в прилагаемой формуле изобретения термин "процессор" должен пониматься как применимый к единственному процессору, так и к двум или более процессорам в сочетании друг с другом.

Используемы здесь и в прилагаемой формуле изобретения термин "память" должен пониматься как применимый к единственной памяти или запоминающему устройству, так и к двум или более памятям или запоминающим устройствам.

Блок-схемы последовательности операций и их описания здесь не должны пониматься как устанавливающие фиксированный порядок выполнения этапов способа, описанного здесь. Напротив, этапы способа могут выполняться в любом порядке, который является практически выполнимым.

Используемы здесь и в прилагаемой формуле изобретения термин "счет в платежной системе" включает в себя счет по кредитной карте или депозитный счет, к которому

держатель счета может иметь доступ, используя дебетовую карту. Термины "счет в платежной системе", "платежный счет" и "счет на платежной карте" используются здесь взаимозаменяемо. Термин "номер платежного счета" включает в себя номер, который идентифицирует счет в платежной системе или номер, носимый платежной картой, или же номер, который используется для направления транзакции в платежной системе, которая обрабатывает транзакции по дебетовой карте и/или кредитной карте. Термин "платежная карта" включает в себя кредитную карту, дебетовую карту или предоплаченную карту.

Используемы здесь и в прилагаемой формуле изобретения термин "платежная система" относится к системе для обработки покупочных транзакций и связанных с ними транзакций. Примером такой системы является та, что управляется MasretCard International Incorporated, правообладателем настоящей раскрываемой информации. В некоторых вариантах осуществления термин "платежная система" может быть ограничен системами, в которых ряд финансовых институтов выпускают платежные счета отдельным лицам, бизнесам и/или другим организациям.

Хотя настоящее изобретение было описано в связи с конкретными приводимыми в качестве примера вариантами осуществления, должно быть понятно, что различные изменения, замены и переделки, понятные для специалистов в данной области техники, могут быть сделаны применительно к описанным вариантам осуществления без отклонения от сущности и объема изобретения, изложенных в прилагаемой формуле изобретения.

(57) Формула изобретения

1. Способ аутентификации бесконтактного платежного устройства с интегральной схемой (IC), который содержит этапы, на которых:

устанавливают канал связи между мобильным устройством и служебным компьютером, поддерживающим дистанционные платежи;

подносят бесконтактное платежное устройство с IC близко к мобильному устройству;

осуществляют обмен данными между бесконтактным платежным устройством с IC и мобильным устройством, причем осуществление обмена содержит транзакцию с нулевой суммой по счету на платежной карте;

генерируют криптограмму в бесконтактном платежном устройстве с IC;

передают криптограмму от бесконтактного платежного устройства с IC в мобильное устройство;

принимают криптограмму в мобильном устройстве;

передают криптограмму от мобильного устройства в служебный компьютер, поддерживающий дистанционные платежи;

осуществляют валидацию криптограммы посредством служебного компьютера, поддерживающего дистанционные платежи, и аутентифицируют бесконтактное платежное устройство с IC, если криптограмма валидирована; и

выдают платежное удостоверение от служебного компьютера, поддерживающего дистанционные платежи, мобильному устройству в ответ на аутентификацию бесконтактного платежного устройства с IC, причем платежное удостоверение связано с платежным счетом, принадлежащим пользователю мобильного устройства, и включает в себя номер основного счета (PAN) или платежный токен,

при этом выдача платежного удостоверения содержит этап, на котором сохраняют PAN или платежный токен, соответственно, в элементе безопасности в мобильном устройстве или в защищенном удаленном хост-сервере.

2. Способ по п. 1, в котором мобильное устройство является устройством, выбираемым из группы, состоящей из: (a) смартфона; (b) планшетного компьютера; (c) персонального компьютера; и (d) умных часов.

3. Способ по п. 1, в котором бесконтактное платежное устройство с IC является имеющим форму карты объектом.

4. Способ по п. 3, в котором бесконтактное IC платежное устройство является устройством, выбираемым из группы, состоящей из: (a) бесконтактной платежной карты; и (b) устройства, соответствующего стандарту, который регламентирует бесконтактные платежные карты.

5. Способ по п. 1, в котором платежный счет доступен представлением бесконтактного IC платежного устройства в пункте продажи.

6. Способ по п. 1, в котором осуществление обмена между бесконтактным IC платежным устройством и мобильным устройством дополнительно содержит транзакцию, отличающуюся от транзакции с нулевой суммой.

7. Способ по п. 1, в котором осуществление обмена между бесконтактным IC платежным устройством и мобильным устройством выполняется в соответствии с NFC стандартом связи.

8. Способ по п. 1, который дополнительно содержит:

ответ в служебном компьютере, поддерживающем дистанционные платежи, на прием криптограммы утверждением покупочной транзакции электронной торговли.

9. Мобильное устройство для аутентификации бесконтактного платежного устройства с интегральной схемой (IC), которое содержит:

процессор; и

память, связанную с процессором, причем эта память содержит программные команды, которые исполняет процессор для выполнения следующих функций:

установления канала связи со служебным компьютером, поддерживающим дистанционные платежи;

обмена данными с бесконтактным платежным устройством с IC, причем обмен данными содержит транзакцию с нулевой суммой по счету на платежной карте;

запуска бесконтактного платежного устройства с IC для генерации криптограммы;

приема криптограммы от бесконтактного платежного устройства с IC;

передачи принятой криптограммы в служебный компьютер, поддерживающий дистанционные платежи;

приема платежного удостоверения от служебного компьютера, поддерживающего дистанционные платежи, в случае, если криптограмма валидирована посредством служебного компьютера, поддерживающего дистанционные платежи, и бесконтактное платежное устройство с IC аутентифицировано,

причем платежное удостоверение связано с платежным счетом, принадлежащим пользователю мобильного устройства, и включает в себя номер основного счета (PAN) или платежный токен,

при этом мобильное устройство дополнительно содержит элемент безопасности, выполненный с возможностью сохранения данных, и при приеме платежного удостоверения PAN или платежный токен, соответственно, сохраняется в элементе безопасности или в защищенном удаленном хост-сервере.

10. Мобильное устройство по п. 9, причем обмен данными с бесконтактным платежным устройством с IC дополнительно содержит транзакцию, которая не является транзакцией с нулевой суммой.

11. Способ аутентификации бесконтактного платежного устройства с интегральной

схемой (IC), который содержит этапы, на которых:

устанавливают канал связи с мобильным устройством;

принимают криптограмму от мобильного устройства, причем криптограмма переправляется мобильным устройством от бесконтактного IC платежного устройства, которое взаимодействует с мобильным устройством;

в ответ на прием и валидацию криптограммы аутентифицируют бесконтактное платежное устройство с IC; и

в ответ на аутентификацию бесконтактного платежного устройства с IC выдают платежное удостоверение мобильному устройству, причем платежное удостоверение связано с платежным счетом, принадлежащим пользователю мобильного устройства, и включает в себя номер основного счета (PAN) или платежный токен,

при этом выдача платежного удостоверения содержит этап, на котором сохраняют PAN или платежный токен, соответственно, в элементе безопасности в мобильном устройстве или в защищенном удаленном хост-сервере.

12. Способ по п. 11, который дополнительно содержит этап, на котором:

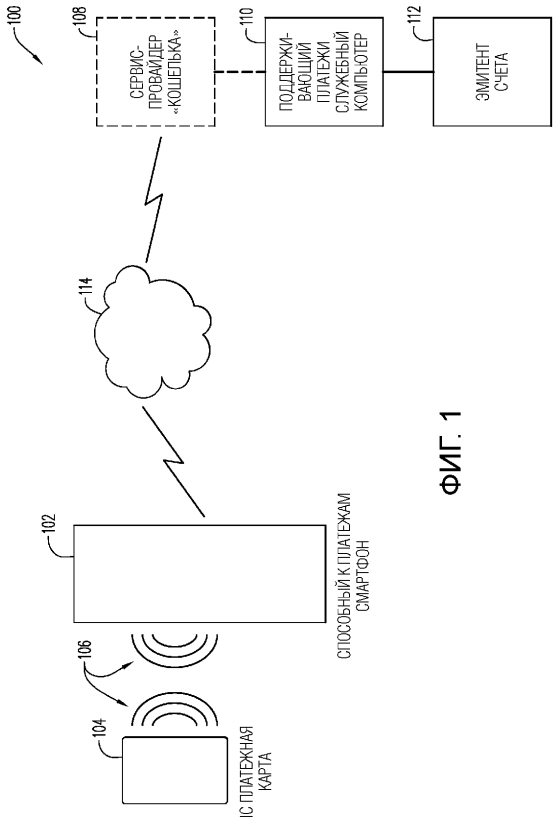
до упомянутого этапа выдачи получают согласие на упомянутый этап выдачи от эмитента бесконтактного IC платежного устройства.

13. Способ по п. 12, причем упомянутое получение согласия включает в себя передачу PAN и криптограммы эмитенту бесконтактного IC платежного устройства.

1

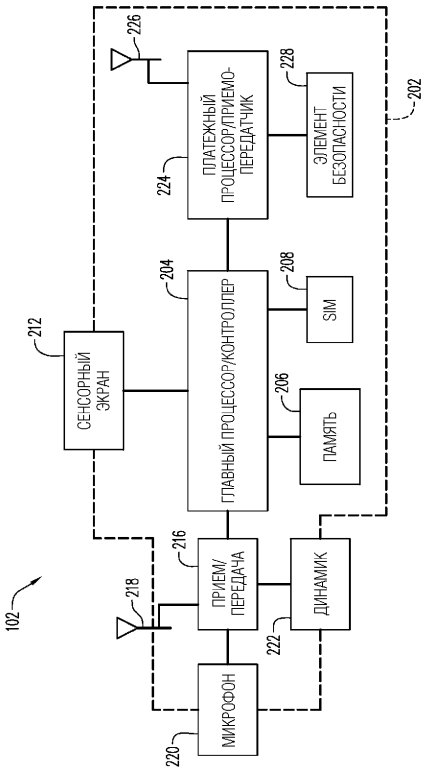
545878

1/5



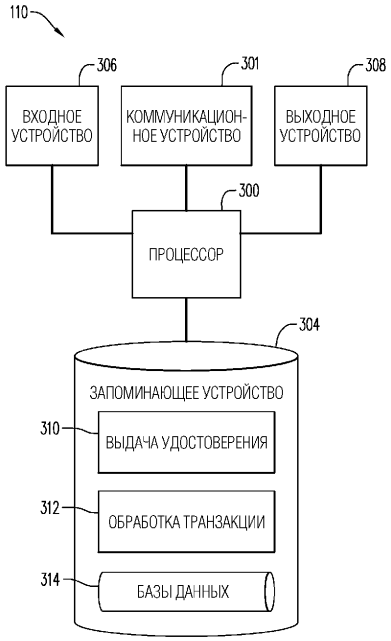
ФИГ. 1

2


102
202
204
206
208
212
216
218
220
222
224
226
228
ГЛАВНЫЙ ПРОЦЕССОР/КОНТРОЛЛЕР
ПАМЯТЬ
SIM
СЕНСОРНЫЙ ЭКРАН
ПРИЕМ/ ПЕРЕДАЧА
ДИНАМИК
МИКРОФОН
ПЛАТЕЖНЫЙ ПРОЦЕССОР/ПРИЕМО-ПЕРЕДАТЧИК
ЭЛЕМЕНТ БЕЗОПАСНОСТИ

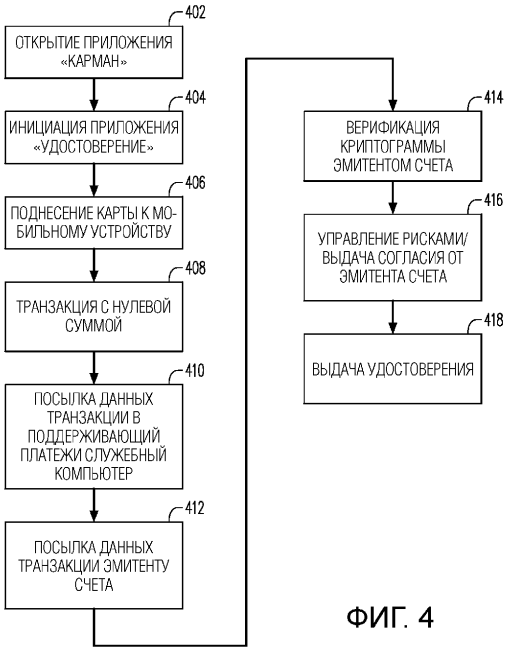
ФИГ. 2

3


110
306
301
308
ВХОДНОЕ УСТРОЙСТВО
КОММУНИКАЦИОННОЕ УСТРОЙСТВО
ВЫХОДНОЕ УСТРОЙСТВО
300
ПРОЦЕССОР
304
ЗАПОМИНАЮЩЕЕ УСТРОЙСТВО
310
ВЫДАЧА УДОСТОВЕРЕНИЯ
312
ОБРАБОТКА ТРАНЗАКЦИИ
314
БАЗЫ ДАННЫХ

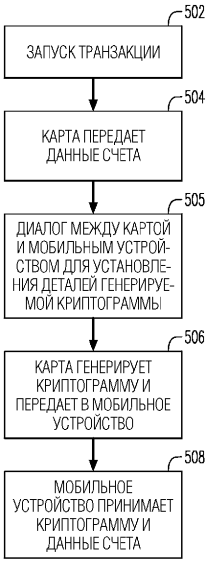
ФИГ. 3

4


402
ОТКРЫТИЕ ПРИЛОЖЕНИЯ «КАРМАН»
404
ИНИЦИАЦИЯ ПРИЛОЖЕНИЯ «УДОСТОВЕРЕНИЕ»
406
ПОДНЕСЕНИЕ КАРТЫ К МОБИЛЬНОМУ УСТРОЙСТВУ
408
ТРАНЗАКЦИЯ С НУЛЕВОЙ СУММОЙ
410
ПОСЫЛКА ДАННЫХ ТРАНЗАКЦИИ В ПОДДЕРЖИВАЮЩИЙ ПЛАТЕЖИ СЛУЖЕБНЫЙ КОМПЬЮТЕР
412
ПОСЫЛКА ДАННЫХ ТРАНЗАКЦИИ ЭМИТЕНТУ СЧЕТА
414
ВЕРИФИКАЦИЯ КРИПТОГРАММЫ ЭМИТЕНТОМ СЧЕТА
416
УПРАВЛЕНИЕ РИСКАМИ/ ВЫДАЧА СОГЛАСИЯ ОТ ЭМИТЕНТА СЧЕТА
418
ВЫДАЧА УДОСТОВЕРЕНИЯ

ФИГ. 4

5


502
ЗАПУСК ТРАНЗАКЦИИ
504
КАРТА ПЕРЕДАЕТ ДАННЫЕ СЧЕТА
505
ДИАЛОГ МЕЖДУ КАРТОЙ И МОБИЛЬНЫМ УСТРОЙСТВОМ ДЛЯ УСТАНОВЛЕНИЯ ДЕТАЛЕЙ ГЕНЕРИРУЕМОЙ КРИПТОГРАММЫ
506
КАРТА ГЕНЕРИРУЕТ КРИПТОГРАММУ И ПЕРЕДАЕТ В МОБИЛЬНОЕ УСТРОЙСТВО
508
МОБИЛЬНОЕ УСТРОЙСТВО ПРИНИМАЕТ КРИПТОГРАММУ И ДАННЫЕ СЧЕТА

ФИГ. 5