(19) Евразийское патентное ведомство

(11) 041883 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.12.12

(21) Номер заявки
201691800

(22) Дата подачи заявки
2015.03.24

(51) Int. Cl. *G06Q 20/32* (2012.01)

(54) СИСТЕМА И СПОСОБ ДЛЯ ПРОВЕДЕНИЯ УДАЛЕННЫХ ТРАНЗАКЦИЙ С ИСПОЛЬЗОВАНИЕМ ПЛАТЕЖНОГО ТЕРМИНАЛА ТОЧКИ ПРОДАЖ

(31) **14/224,461; 1503586.8**
(32) **2014.03.25; 2015.03.03**
(33) **US; GB**
(43) **2017.03.31**
(86) **PCT/GB2015/050869**
(87) **WO 2015/145131 2015.10.01**

(71)(73) Заявитель и патентовладелец:
АЙАКСЕПТ ЛИМИТЕД (GB)

(72) Изобретатель:
Саволайнен Ристо, Джайет Стефан (GB)

(74) Представитель:
Хмара М.В., Рыбаков В.М., Липатова И.И., Новоселова С.В., Дощечкина В.В., Пантелеев А.С., Ильмер Е.Г., Осипов К.В. (RU)

(56) Wikipedia: "Credit card terminal", INTERNET ARTICLE, 14 March 2014 (2014-03-14), XP055193148, Retrieved from the Internet: URL:https://en.wikipedia.org/w/index.php?title=Credit_card_terminal&oldid=599603358 [retrieved on 2015-06-02] the whole document

Sarah Perez: "CHARGE Anywhere Makes Nexus S an NFC Terminal", INTERNET ARTICLE, 28 March 2011 (2011-03-28), XP055178768, Retrieved from the Internet: URL:http://readwrite.com/2011/93/28/Charge_Anywhere_makes_nexus_s_an_nfc_terminal [retrieved on 2015-03-24] the whole document

Mastercard: "MASTERCARD BEST PRACTICES FOR MOBILE POINT OF SALE ACCEPTANCE - A Guide to Enabling Acceptance on Mobile Devices", INTERNET ARTICLE, 22 November 2013 (2013-11-22), XP055193367, Retrieved from the Internet: URL:http://www.mastercard.com/corporate/_assets/img/features/MasterCard_Mobile_Point_of_Sale_Best_Practices.pdf [retrieved on 2015-06-03] page 4

Herminia Suarez: "CHARGE Anywhere Achieves MasterCard Mobile Point-of-Sale Program (MPOS) Compliance for EMV MPOS Solution", Reuters.com INTERNET ARTICLE, 21 May 2013 (2013-05-21), XP055193604, Retrieved from the Internet: URL:http://www.reuters.com/article/2013/05/21/nj-charge-anywhere-idUSnBw216749a+100+BSW20130521 [retrieved on 2015-06-03] the whole document

Mastercard: "Mobile POS Self-certified Solution Providers", INTERNET ARTICLE, 26 November 2013 (2013-11-26), XP055193601, Retrieved from the Internet: URL:http://www.mastercard.com/corporate/_assets/img/features/MPOSApprovedSolutions.pdf [retrieved on 2015-06-03] the whole document

WO-A2-2010128442
US-A1-2014013406
US-A1-2014074637

Wikipedia: "Public key infrastructure", INTERNET ARTICLE, 24 March 2014 (2014-03-24), XP055193186, Retrieved from the Internet: URL:https://en.wikipedia.org/w/index.php?title=Public_key_infrastructure&oldid=601049646 [retrieved on 2015-06-02] the whole document

Josef Langer et al.: "Anwendungen und Technik Von Near Field Communication (NFC)" In: "Anwendungen und Technik von Near Field Communication (NFC)", 16 September 2010 (2010-09-16), Springer Berlin Heidelberg, Berlin, Heidelberg, XP055178840, ISBN: 978-3-64-205497-6 Ch01, Ch05, Ch07-Ch09

(57) Раскрыты система обработки удаленных транзакций, способ и терминал точки продаж. Указанная система содержит первое хранилище данных. Первое хранилище данных содержит профиль пользовательского устройства, относящийся к пользовательскому устройству и содержащий данные маршрутизации для маршрутизации сообщений в указанное пользовательское устройство. Система обработки удаленных транзакций выполнена с возможностью после приема запроса платежа, задающего пользовательское устройство для выполнения транзакции с продавцом, получения профиля конфигурации точки продаж, соответствующего указанному продавцу, и получения профиля пользовательского устройства из первого хранилища данных, соответствующего этому заданному пользовательскому устройству. Система обработки удаленных транзакций выполнена с возможностью сообщения конфигурации точки продаж, соответствующей указанному профилю конфигурации точки продаж, в пользовательское устройство в соответствии

041883 B1

041883 B1

с указанными данными маршрутизации, а указанная конфигурация точки продаж может быть выполнена указанным пользовательским устройством с целью придания этому пользовательскому устройству возможности использования в качестве терминала точки продаж для осуществления указанной транзакции с указанным продавцом.

041883 B1

041883 B1

Область техники, к которой относится изобретение

Настоящее изобретение относится к системе, способу и терминалу точки продаж (Point-of-Sale, PoS), применимым, в частности, в транзакциях, в которых покупатель удален от продавца.

Уровень техники

Онлайновые магазины и продавцы часто в качестве средства платежа принимают кредитные и дебитные карты. Одним недостатком онлайн платежей с использованием карты является то, что пользователь должен вручную вводить информацию карты в поля на странице веб-сайта интернет-магазина или на странице, связанной с указанным веб-сайтом.

Вышеописанный онлайн платеж с использованием карты является так называемой транзакцией без предъявления карты, поскольку в момент транзакции продавец не имеет возможности проверить существование физической карты. Транзакции без предъявления карты могут быть легко сфальсифицированы и риск для продавца является высоким. Как следствие, высоким является соответствующий комиссионный сбор за транзакцию.

Например, нет гарантии, что пользователь вводит информацию своей карты, т.е. информация карты может быть похищена или получена иным противозаконным образом, и ее использование может привести к финансовым потерям продавца и/или покупателя. Информация, передаваемая на указанный веб-сайт, может быть злонамеренно использована для проведения мошеннических транзакций любым лицом, имеющим доступ к этой информации, или "человеком посередине", имеющим возможность выделять эту информацию из данных, передаваемых между пользователем и указанным веб-сайтом. Это может быть реализовано несколькими способами.

Для защиты транзакций без предъявления карты были предложены различные способы. Часто эти способы не дают существенного повышения защищенности или требуют значительной модификации существующей инфраструктуры и веб-сайтов вследствие несовместимости с существующими системами. Типовые терминалы точки продаж непригодны для использования конечными пользователями у себя дома или в иных местах для проведения транзакций без предъявления карты, поскольку каждый терминал точки продаж настроен под конкретного продавца. Когда покупатель выполняет платеж в магазине, терминал точки продаж переводит этот платеж на заранее заданный банковский счет. Идея того, что для каждого отдельного интернет-продавца каждый покупатель должен иметь терминал точки продаж, который этот покупатель мог бы использовать для совершения платежа с переводом на соответствующий этому продавцу банковский счет, нереалистична.

Сущность изобретения

В соответствии с аспектом настоящего изобретения предлагается система обработки удаленных транзакций, содержащая первое хранилище данных, содержащее профиль пользовательского устройства, относящийся к пользовательскому устройству и содержащий данные маршрутизации для маршрутизации связи в пользовательское устройство; причем система выполнена с возможностью при приеме запроса платежа, задающего пользовательское устройство для выполнения транзакции с продавцом, получения профиля конфигурации точки продаж, соответствующей продавцу, и получения из первого хранилища данных профиля пользовательского устройства, соответствующего указанному заданному пользовательскому устройству, и с возможностью сообщения конфигурации точки продаж, зависящей от профиля конфигурации точки продаж, в пользовательское устройство в зависимости от данных маршрутизации, при этом конфигурация точки продаж выполняется пользовательским устройством с целью обеспечения пользовательскому устройству возможности использования в качестве терминала точки продаж для выполнения транзакции с продавцом.

Предпочтительно профиль пользовательского устройства содержит открытый ключ из криптографической пары ключей пользовательского устройства, а система обработки удаленных транзакций выполнена с возможностью шифрования сообщаемой конфигурации точки продаж с использованием открытого ключа.

Предпочтительно данные маршрутизации содержат множество маршрутов для осуществления связи с пользовательским устройством, а система обработки удаленных транзакций выполнена с возможностью определения маршрута из числа множества маршрутов для осуществления связи с пользовательским устройством.

Маршрутам в данных маршрутизации могут назначаться ранги, а система обработки удаленных транзакций может быть выполнена с возможностью идентификации маршрута для достижения пользовательского устройства в зависимости от указанных рангов.

Предпочтительно маршруты включают маршруты для осуществления связи с пользовательским устройством через различные каналы.

Каналы могут быть выбраны из множества, содержащего SMS, мгновенные сообщения, связь с заранее определенным адресом в сети передачи данных или вызов для передачи данных по сети связи.

Система может дополнительно содержать второе хранилище данных, содержащее профиль конфигурации точки продаж для каждого продавца из множества продавцов, и может быть выполнена с возможностью получения профиля конфигурации точки продаж для продавца из второго хранилища данных.

Второе хранилище данных может содержать сертификат точки продаж, относящийся к соответствующему продавцу и содержащий профиль конфигурации точки продаж продавца.

Первое хранилище данных может содержать сертификат пользовательского устройства, относящийся к соответствующему пользовательскому устройству и содержащий открытый ключ пользовательского устройства.

Первое и второе хранилища данных могут быть одним и тем же хранилищем данных.

Первое хранилище данных может содержать профиль пользовательского устройства для каждого пользовательского устройства из множества пользовательских устройств.

Первое хранилище данных может быть удаленным по отношению к пользовательским устройствам.

Первое хранилище данных может быть локальным по отношению к пользовательскому устройству, таким образом, профиль пользовательского устройства можно получить из указанного пользовательского устройства.

Система может содержать веб-сайт продавца, содержащий платежный пользовательский интерфейс, реализованный с возможностью приема от пользователя идентификатора, указывающего профиль пользовательского устройства, которое должно использоваться для платежа, при этом система может быть выполнена с возможностью получения профиля пользовательского устройства в зависимости от указанного идентификатора.

Система может содержать систему обработки платежей, выполненную с возможностью приема запросов платежа для каждого продавца из множества продавцов.

Система обработки платежей может быть выполнена с возможностью приема профиля конфигурации точки продаж от продавца при приеме запроса платежа.

Система может содержать пользовательское устройство, которое содержит прикладную программу терминала точки продаж и считыватель платежных карт, при этом пользовательское устройство может быть выполнено с возможностью приема конфигурации точки продаж для транзакции с продавцом, с возможностью конфигурирования прикладной программы терминала точки продаж в зависимости от указанной конфигурации точки продаж и с возможностью считывания платежной карты посредством считывателя платежных карт для выполнения платежа по данной транзакции посредством прикладной программы терминала точки продаж.

Пользовательское устройство может содержать защищенный элемент, в котором выполняется прикладная программа терминала точки продаж, выбираемый из множества, содержащего модуль идентификации абонента (SIM), универсальная карта с интегральной схемой (UICC) или встроенный защищенный элемент (ESE), доверенную среду исполнения (TEE) или защищенную среду.

Защищенный элемент может быть вставлен, вмонтирован или встроен в пользовательское устройство.

В соответствии с еще одним аспектом настоящего изобретения предлагается способ обработки удаленных транзакций, включающий прием запроса платежа, задающего пользовательское устройство для выполнения транзакции с продавцом; получение профиля конфигурации точки продаж, соответствующего продавцу; получение профиля пользовательского устройства, соответствующего указанному заданному пользовательскому устройству и содержащего данные маршрутизации для маршрутизации связи в пользовательское устройство; и сообщение конфигурации точки продаж, зависящей от профиля конфигурации точки продаж, в пользовательское устройство в зависимости от данных маршрутизации, при этом конфигурация точки продаж выполняется пользовательским устройством с целью обеспечения пользовательскому устройству возможности использования в качестве терминала точки продаж для выполнения транзакции с продавцом.

Указанный способ может дополнительно включать связывание криптографического сертификата, содержащего открытый ключ из пары открытого и секретного ключей, с профилем пользовательского устройства; шифрование по меньшей мере части конфигурации точки продаж с использованием открытого ключа и расшифровку зашифрованной конфигурации точки продаж в пользовательском устройстве с использованием секретного ключа.

Указанный способ может дополнительно включать сохранение криптографического сертификата в хранилище данных, а шаг получения профиля пользовательского устройства может включать получение указанного сертификата.

Шаг приема запроса платежа может включать прием информации о транзакции, а шаг сообщения конфигурации точки продаж может включать формирование конфигурации точки продаж в зависимости от информации о транзакции и профиля конфигурации точки продаж.

Шаг формирования конфигурации точки продаж может включать подписывание конфигурации точки продаж с использованием секретного ключа из криптографической пары секретного и открытого ключей.

Указанный способ может дополнительно включать выполнение в пользовательском устройстве следующих шагов: выполнение транзакции карточного платежа в пользовательском устройстве посредством терминала точки продаж; подписывание в терминале точки продаж данных транзакции платежа; шифрование в терминале точки продаж подписанных данных транзакции платежа; передачу терминалом

точки продаж зашифрованных и подписанных данных транзакции платежа в узел платежного сервиса; и удаление терминалом точки продаж указанной информации платежа из памяти терминала точки продаж. В одном или большем числе вариантов осуществления предлагается способ защиты всей связи в обоих направлениях с удаленно конфигурируемой системой терминала точки продаж и удаленно конфигурируемая система терминала точки продаж. Указанный способ включает использование криптографических ключей терминала точки продаж и узла платежной системы продавца, использующего криптографический ключ терминала точки продаж для шифрования информации платежа на основании введенных данных транзакции. Указанный способ также включает подписывание сформированной информации платежа секретным ключом и передачу подписанной информации платежа. Продавец или организация, предоставляющая продавцу платежный сервис, конфигурирует терминал точки продаж посредством собственного профиля терминала точки продаж продавца на основании инструкций, переданных в информации платежа.

В одном или большем числе вариантов осуществления предлагается способ удаленного конфигурирования терминала точки продаж. Указанный способ включает прием в терминале точки продаж подписанной информации платежа. Указанный способ также включает проверку в терминале точки продаж действительности информации платежа с использованием сертификата открытого ключа.

В одном или большем числе вариантов осуществления предлагается способ удаленного конфигурирования терминала точки продаж. Указанный способ включает прием в устройстве продавца введенных данных транзакции. Указанный способ также включает формирование в устройстве продавца информации платежа на основании введенных данных транзакции и подписывание сформированной информации платежа секретным ключом. Способ дополнительно включает передачу подписанной информации платежа и сертификата открытого ключа, подписанного удостоверяющим центром, в терминал точки продаж. Способ включает проверку в терминале точки продаж действительности сертификата открытого ключа с использованием сертификата открытого ключа удостоверяющего центра и действительности информации платежа с использованием сертификата открытого ключа, подписанного удостоверяющим центром. Указанный способ также включает конфигурирование в терминале точки продаж профиля терминала указанного терминала точки продаж в соответствии с инструкциями, принятыми в информации платежа, если эта информация платежа успешно прошла проверку действительности в терминале точки продаж.

Информация платежа и первый сертификат открытого ключа до передачи подписанной информации платежа и первого сертификата открытого ключа с использованием сертификата второго открытого ключа терминала точки продаж или банка-эквайера.

Краткое описание чертежей

Далее со ссылкой на сопровождающие чертежи лишь посредством примера описываются варианты осуществления настоящего изобретения. На этих чертежах

фиг. 1 представляет собой схему системы обработки удаленных транзакций в соответствии с вариантом осуществления настоящего изобретения;

фиг. 2 - схему элементов системы, показанной на фиг. 1, в работе;

фиг. 3 - иллюстрацию последовательности операций в транзакции с продавцом, передающим информацию платежа в мобильное пользовательское устройство, выполняющее прикладную программу точки продаж (и тем самым ставшее терминалом точки продаж);

фиг. 4 - схему, иллюстрирующую выдачу допуска защиты и конфигурирование профиля терминала временной точки продаж без использования банка-эквайера;

фиг. 5 - сообщения в транзакции с удаленным покупателем с использованием отдельного терминала для совершения покупок и мобильного устройства для платежа; и

фиг. 6 - сообщения в транзакции с удаленным покупателем с использованием мобильного устройства как для совершения покупок, так и для платежа.

Сведения, подтверждающие возможность осуществления изобретения

Далее подробно рассматриваются предпочтительные варианты осуществления настоящего изобретения, примеры которых представлены на сопровождающих чертежах, где подобные ссылочные обозначения повсеместно относятся к подобным элементам.

Фиг. 1 представляет собой схему системы обработки удаленных транзакций в соответствии с вариантом осуществления настоящего изобретения.

Система 10 обработки удаленных транзакций содержит первое хранилище 20 данных.

Первое хранилище 20 данных содержит профиль пользовательского устройства для каждого пользовательского устройства из множества пользовательских устройств, а каждый профиль пользовательского устройства содержит данные маршрутизации для маршрутизации сообщений в это пользовательское устройство.

Система 10 обработки удаленных транзакций выполнена с возможностью при приеме запроса платежа, задающего пользовательское устройство 40 устройством для проведения транзакции с продавцом, получения профиля конфигурации точки продаж, соответствующего указанному продавцу, и получения профиля пользовательского устройства из первого хранилища 20 данных, соответствующего этому за-

данному пользовательскому устройству 40. Система 10 обработки удаленных транзакций сообщает конфигурацию точки продаж, соответствующую указанному профилю конфигурации точки продаж, в пользовательское устройство 40 через сеть 30 передачи данных в соответствии с указанными данными маршрутизации. Указанная конфигурация точки продаж может быть выполнена пользовательским устройством 40 с целью придания этому пользовательскому устройству возможности использования в качестве терминала точки продаж для выполнения указанной транзакции с указанным продавцом.

В качестве одной из возможностей система 10 обработки удаленных транзакций может содержать второе хранилище данных. Это второе хранилище данных содержит профиль конфигурации точки продаж для каждого продавца из множества продавцов, а система 10 обработки удаленных транзакций обращается к второму хранилищу данных для получения профиля конфигурации точки продаж определенного продавца.

Первое и второе хранилища данных могут быть раздельными или объединенными. Также могут использоваться распределенные и дублированные хранилища данных.

Предпочтительно каждый из профилей конфигурации точки продаж и профилей пользовательского устройства представляет собой или содержит криптографический сертификат, например сертификат PKI (Public Key Infrastructure, инфраструктура открытых ключей). Примеры данных, которые могут содержаться в этих криптографических сертификатах, рассматриваются ниже.

Фиг. 2 представляет собой схему элементов системы, показанной на фиг. 1, в работе.

Пользовательское устройство 40 в данном варианте осуществления представляет собой смартфон и содержит процессор 41, память 42, считыватель 45 карт и дисплей 43. Пользовательское устройство 40 выполнено с возможностью осуществления связи с сетью 30 передачи данных.

Пользователь, взаимодействуя с веб-сайтом 60, доходит до этапа, на котором возникает необходимость совершения платежа в удаленной транзакции с продавцом, связанным с данным веб-сайтом. В настоящем варианте осуществления пользователь обращается к веб-сайту 60 через компьютерное устройство 70, отличное от пользовательского устройства 40, однако должно быть понятно, что пользователь может обращаться к веб-сайту 60 и через пользовательское устройство 40.

Веб-сайт 60 в пользовательском интерфейсе представляет пользователю варианты платежа. Вместо обычного на этом этапе транзакции ввода информации кредитной карты или дебитной карты пользователь вводит идентификатор пользовательского устройства 40.

Приняв этот идентификатор, веб-сайт 60 сообщает его и идентификатор продавца в систему 80 обработки платежей.

Система 80 обработки платежей обращается к первому хранилищу 20 данных для получения профиля конфигурации точки продаж, соответствующего указанному идентификатору продавца, и к второму хранилищу данных 30 для получения профиля пользовательского устройства, соответствующего указанному идентификатору продавца.

Затем система 80 обработки платежей на основании полученного профиля конфигурации точки продаж формирует конфигурацию 90 точки продаж, которую сообщает в пользовательское устройство 40 с использованием данных маршрутизации из полученного профиля пользовательского устройства.

После приема конфигурации 90 точки продаж процессор 41 пользовательского устройства 40 запускает в своей памяти 42 прикладную программу 44 терминала точки продаж и применяет конфигурацию 90 точки продаж, в результате чего пользовательское устройство 40 начинает работать как терминал точки продаж для данного продавца. Пользователю предлагается представить платежную карту в считыватель 45 карт, и данные из представленной карты обрабатываются указанным терминалом точки продаж и сообщаются в систему 100 обработки платежей для завершения транзакции. На данном этапе для системы 80 обработки платежей транзакция выглядит инициированной из терминала точки продаж продавца, почти так же, как если бы она была полностью совершена в магазине с использованием собственного терминала точки продаж данного продавца.

Данные маршрутизации предпочтительно содержат множество маршрутов для осуществления связи с пользовательским устройством 40. Система 80 обработки платежей предпочтительно выполнена с возможностью выбора из указанного множества маршрутов маршрута для осуществления связи с указанным пользовательским устройством. Например, маршрутам в указанных данных маршрутизации могут быть назначены ранги (или в момент необходимости их использования маршруты могут быть проанализированы для назначения рангов). Система 80 обработки платежей может быть выполнена с возможностью определения маршрута к каждому пользовательскому устройству в соответствии с указанными рангами.

В число маршрутов предпочтительно входят маршруты для осуществления связи с пользовательским устройством по разным каналам. Например, указанные каналы могут быть выбраны из множества, содержащего SMS, мгновенные сообщения, передачу на заранее определенный адрес в сети передачи данных или вызов для передачи данных по сети связи.

Например, профиль пользовательского устройства может задавать адрес в программе обмена сообщениями Google в качестве предпочтительного маршрута, адрес в Skype в качестве первого резерва и номер мобильного устройства для передачи SMS в качестве второго резерва. При необходимости сооб-

щения профиля точки продаж система 80 обработки платежей сначала предпринимает попытку осуществить связь с пользовательским устройством через программу обмена сообщениями Google, затем пытается сделать это через Skype и, наконец, отправляет сообщение SMS. При использовании SMS и других способов связи с ограниченным объемом полезной информации возможна отправка множества сообщений или в сообщении может содержаться ссылка или другие параметры, адресующие пользовательское устройство за получением профиля точки продаж.

Данные маршрутизации могут содержать номер MSISDN (номер телефона, Mobile Subscriber Integrated Services Digital Number, номер мобильного абонента цифровой сети с интеграцией служб), псевдоним, идентификатор устройства (например, IMEI, International Mobile Equipment Identity, международный идентификатор мобильного оборудования), идентификатор защищенного элемента (например, IMSI, International Mobile Subscriber Identity, международный идентификатор мобильного абонента), адрес электронной почты, адрес в интернете, адрес в цифровой сети связи или адрес Bluetooth данного пользовательского устройства.

Профиль конфигурации точки продаж может быть в форме сертификата или может содержать сертификат и может, например, содержать один или более из следующих элементов: криптографическую подпись, удостоверяющую содержание сертификата; банковские данные и/или данные обработки платежа для использования прикладной программой терминала точки продаж при передаче информации транзакции, например деталей платежа, в систему 80 обработки платежей.

Конфигурация точки продаж может содержать информацию, подлежащую использованию прикладной программой терминала точки продаж на пользовательском устройстве для того, чтобы установить, необходим ли успешный результат верификации держателя карты для проведения транзакции, связанной с принятой информацией платежа.

Конфигурация точки продаж может содержать информацию о поддерживаемых способах верификации держателя карты.

Конфигурация точки продаж может содержать информацию платежа, содержащую один или более из следующих элементов: дата, время, сумма, валюта, лимит авторизации, лимит при бесконтактном платеже, лимит транзакции, идентификатор транзакции, наименование продавца и страна продавца.

Профиль конфигурации точки продаж может содержать один или более из следующих элементов: идентификатор организации, предоставляющей платежный сервис (Payment Service Provider Identification, PSPID), код идентификации продавца (Merchant Identification, MID) и/ или код идентификации терминала (Terminal Identification, TID).

Профиль пользовательского устройства может быть в форме сертификата или содержать сертификат и может содержать один или более из следующих элементов: открытый ключ из пары криптографических ключей пользовательского устройства, идентификатор IMSI пользовательского устройства, номер MSISDN (номер телефона) пользовательского устройства, идентификатор организации, предоставляющей услугу доступа к сотовой сети, идентификатор защищенного элемента, идентификатор мобильного устройства, разрешенные валюты, запрещенные валюты, признак покупки высокой стоимости с поддержкой верификации держателя карты, наибольшая стоимость покупки, наименьшая стоимость покупки, период действия, информация идентификации разрешенного мобильного устройства, список поддерживаемых видов карт, номер версии прикладной программы точки продаж, информация управления финансовым риском.

Предпочтительно указанным пользовательским устройством является мобильное устройство, например мобильный телефон, смартфон, планшет или другое компьютерное устройство. Указанным пользовательским устройством может быть многоцелевое устройство (например, смартфон с соответствующей прикладной программой или иным аппаратным, программным или микропрограммным решением, придающим этому смартфону возможность использования в качестве терминала точки продаж), или специализированное устройство для предоставления пользователю функций точки продаж при осуществлении удаленных транзакций. Предпочтительно пользовательское устройство содержит считыватель карт, например считыватель данных из чипа, с магнитной полосы, считыватель кода PIN и/ или антенну радиосвязи малого радиуса действия (NFC и т.д.), дисплей, память, процессор, программу, которая может быть выполнена процессором, источник питания, радиочастотный передатчик, антенну мобильной телефонии или другой соединитель с сетью и средство пользовательского ввода, например, клавиатуру, сенсорный экран, камеру и/ или микрофон.

Пара криптографических ключей пользовательского устройства может формироваться в этом пользовательском устройстве или может назначаться этому пользовательскому устройству. Указанная пара криптографических ключей может сохраняться в пользовательском устройстве при его изготовлении.

Пользовательское устройство может осуществлять связь через одну или более сотовую сеть, Bluetooth или другое средство радиочастотной связи на малых расстояниях, интернет, локальную сеть, беспроводную локальную сеть, камеру, встроенную в мобильное устройство, кабель, присоединенный к устройству, микрофон или карту памяти.

Система 80 обработки платежей предпочтительно выполнена с возможностью шифрования сообщаемой конфигурации точки продаж с использованием открытого ключа из указанного профиля пользо-

вательского устройства.

Предпочтительные варианты осуществления дают пользовательскому устройству возможность работы в качестве терминала точки продаж. В предпочтительных вариантах осуществления предоставляется возможность защищенной обработки удаленных транзакций, предпочтительно с использованием профиля продавца, назначаемого лишь временно и сохраняемого в пользовательском устройстве, используемом в качестве терминала точки продаж, что позволяет использовать такой временный профиль продавца только на протяжении конкретной транзакции. Пока временный профиль продавца активирован и используется, пользовательское устройство осуществляет функции терминала точки продаж, работающего как удаленный терминал точки продаж продавца, при этом уплаченная сумма поступает на счет продавца, указанный в этом временном профиле. Когда конкретная транзакция выполнена, этот временный профиль предпочтительно удаляется, соответственно, терминал не может быть использован снова до тех пор, пока он не примет новый профиль и введенные данные транзакции.

Как должно быть понятно, в предпочтительных вариантах осуществления покупателю нигде не нужно вводить информацию своей платежной карты, поэтому информация карты не может быть использована для мошенничества.

Прикладная программа 44 точки продаж может быть осуществлена в соответствии с одновременно находящейся на рассмотрении патентной заявкой США № US 61726121, содержание которой полностью включено в настоящий документ. Прикладная программа 44 может быть реализована аппаратурой, микропрограммой, программой или некоторым их сочетанием и может находиться в карте UICC/SIM. Прикладная программа 44 может соответствовать схеме EMV работы с платежной картой и использовать решение на основе сертификатов защиты типа инфраструктуры открытых ключей (PKI).

Предпочтительные варианты осуществления дают возможность совершения защищенных электронных платежей с использованием чиповых карт или мобильного кошелька. В предпочтительных вариантах осуществления используется прикладная программа (которая может находиться в защищенной памяти чиповой карты или в пользовательском устройстве) точки продаж, имеющей считыватель смарт-карт или интерфейс считывателя карт на основе ближней связи, например радиосвязи малого радиуса действия (Near Field Communication, NFC), и техническую возможность осуществления связи через сеть.

Предпочтительно используются защищенные сертификаты на основе PKI. Целостность цепи управления ключом защиты дает возможность построения и поддержания в системе высоких уровней защищенности.

Управление системой защиты.

Существует несколько сценариев управления системой защиты. В первом из них участвуют продавец, банк-эквайер, удостоверяющий центр (УЦ, например, система карточных платежей) и покупатель. Во втором сценарии участвуют продавец, УЦ и покупатель. В третьем сценарии дополнительно участвует доверенная третья сторона, которая ведет базу данных сертификатов точек продаж.

Пользовательское устройство в качестве одной из возможностей посредством прикладной программы точки продаж формирует и/или использует пару криптографических ключей: защищенный секретный ключ и соответствующий открытый ключ. Указанная пара ключей может относиться только к данной прикладной программе точки продаж или может использоваться и другими прикладными программами, исполняемыми в том же процессоре и/или в том же защищенном элементе.

Пользовательское устройство предпочтительно хранит секретный ключ в защищенной от постороннего вмешательства памяти или в защищенном элементе. Этот способ гарантирует сохранение секретного ключа в абсолютной секретности, поскольку секретный ключ не может быть считан или иным образом сделан явным за пределами защищенного элемента.

Пользовательское устройство предпочтительно создает или использует сертификат открытого ключа (сертификат профиля пользовательского устройства), публикует его и передает в узел внешней базы данных сертификатов (перед первой платежной транзакцией). В варианте осуществления, показанном на фиг. 1, таким узлом (или элементом, осуществляющим связь с таким узлом), является первое хранилище данных, таким образом, сертификат получают из первого хранилища данных. В качестве одной из возможностей получение сертификата может осуществляться непосредственно из пользовательского устройства без сохранения в базе данных.

Как обсуждалось выше, система обработки платежей (например, узел платежного сервиса) выполнена с возможностью получения сертификата мобильного устройства пользователя из базы данных сертификатов с использованием номера MSISDN или аналогичного уникального идентификатора устройства или пользователя.

Система обработки платежей может в качестве одной из возможностей проверять действительность полученного сертификата пользовательского устройства с целью проверки наличия в мобильном устройстве покупателя совместимой прикладной программы точки продаж и наличия у этой программы разрешения на выполнение данной транзакции.

Система обработки платежей предпочтительно использует открытый ключ из сертификата для частичного или полного шифрования информации платежа до передачи этой информации в терминал точки продаж или в шлюзовой узел.

Система обработки платежей может в качестве одной из возможностей содержать информацию маршрутизации возврата, например, сетевой IP-адрес, идентификатор сервера, доменное имя в сообщаемом профиле точки продаж, с целью получения информации об информации транзакции, например запроса авторизации и завершенных транзакций.

Предпочтительно прикладная программа точки продаж на пользовательском устройстве выполнена с возможностью проверки того, что принятый этой программой профиль конфигурации точки продаж продавца действителен и не был изменен. Эта проверка может быть осуществлена с использованием системы защиты на основе PKI, наследующей доверие от общего УЦ. Для этой цели сертификат открытого ключа удостоверяющего центра сообщается в терминал точки продаж (как правило, при изготовлении, но это может быть сделано и позже).

В обоих сценариях перед первым шагом покупатель уже закончил выбор покупок в интернет-магазине, поэтому полная информация платежа известна, пользователь выбрал опцию оплаты с использованием мобильного устройства, обладающего функциональностью защищенного терминала точки продаж, и ввел номер своего мобильного устройства.

Узел продавца предоставляет покупателю средства для ввода номера телефона или другого идентификатора или с этой же целью перенаправляет покупателя на страницу платежа на узле платежного сервиса. Идентификационный код пользователя может сохраняться в данных cookie или аналогичным способом на компьютерном устройстве покупателя и автоматически подставляться в соответствующее поле на странице платежа. Это дает покупателю возможность использовать способ покупки одним щелчком вообще без ввода какой-либо информации кредитной карты.

1. Покупатель на своем мобильном устройстве выбирает способ платежа с использованием удаленного терминала точки продаж.

2. Продавец пересылает информацию платежа в узел платежного сервиса, эксплуатируемый, например, эквайером платежей или организацией, предоставляющей платежный сервис (payment service provider, PSP).

3. Покупатель вводит номер своего мобильного устройства (MSISDN) или аналогичный уникальный идентификатор на странице узла платежного сервиса.

4. Узел платежного сервиса получает сертификат профиля пользовательского устройства из узла базы данных сертификатов, соответствующего введенной покупателем информации.

5. Если это получение прошло успешно, то PSP проверяет действительность сертификата и проверяет, оснащено ли мобильное устройство совместимой версией терминала точки продаж.

6. PSP подписывает информацию платежа.

7. PSP шифрует информацию платежа с использованием открытого ключа терминала точки продаж.

8. Если информация платежа действительна, то точка продаж конфигурирует свой профиль терминала в соответствии с инструкциями, принятыми в указанной информации платежа, на время одной транзакции.

9. Точка продаж представляет указанные инструкции платежа пользователю.

10. Пользователь может согласиться с платежом или отклонить его.

11. Платеж, если получено согласие, будет обрабатываться согласно соответствующему способу.

12. Когда обработка платежа завершена, терминал точки продаж автоматически удаляет свой профиль, и этот терминал больше не может использоваться до тех пор, пока не получит новую информацию платежа.

На фиг. 3 и 4 вариант осуществления настоящего изобретения проиллюстрирован в виде схемы последовательности операций и блок-схемы транзакции. Схема последовательности операций транзакции на фиг. 3 иллюстрирует последовательность операций в транзакции с продавцом, передающим информацию платежа в мобильное пользовательское устройство, выполняющее прикладную программу точки продаж (и тем самым ставшее терминалом точки продаж). Блок-схема транзакции на фиг. 4 представляет схему, иллюстрирующую выдачу допуска защиты и конфигурирование профиля терминала временной точки продаж без использования банка-эквайера. Данная система содержит устройство продавца и удостоверяющий центр, без банка-эквайера. В данном варианте осуществления без банка-эквайера могут иметь место следующие операции.

1. Продавец подписывает информацию платежа (ИП) своим секретным ключом.

2. Продавец передает подписанную ИП и сертификат открытого ключа продавца, подписанный УЦ, в терминал точки продаж.

3. Терминал точки продаж проверяет действительность сертификата открытого ключа продавца с использованием сертификата открытого ключа УЦ.

4. Если сертификат продавца действителен, то точка продаж использует его для проверки действительности ИП.

5. Если ИП действительна, то точка продаж конфигурирует свой профиль терминала в соответствии с инструкциями, принятыми в указанной ИП, на время одной транзакции.

6. Точка продаж представляет указанные инструкции платежа пользователю.

7. Пользователь может согласиться с платежом или отклонить его.

8. Платеж, если получено согласие, будет обрабатываться согласно соответствующему способу.

9. Когда обработка платежа завершена, терминал точки продаж автоматически удаляет свой профиль, и этот терминал больше не может использоваться до тех пор, пока не получит новую информацию платежа.

Также возможны другие сценарии с таким же уровнем защиты, обеспечиваемой непрерывностью цепи сертификатов защиты.

Выбор этих сценариев невидим пользователю. Иными словами, основное отличие в обработке потока данных в мобильные устройства состоит в том, нужна ли продавцам возможность управления передачей данных между своими системами и различными мобильными устройствами, или эта функция сосредоточивается у банков-эквайеров и выполняется ими.

Последовательность сообщений в транзакции.

Фиг. 5 иллюстрирует сообщения в транзакции с удаленным покупателем с использованием отдельного терминала для выбора покупок и мобильного устройства для платежа. Фиг. 6 иллюстрирует сообщения в транзакции с удаленным покупателем с использованием мобильного устройства как для выбора покупок, так и для платежа.

(1) Пользователь, готовый к оплате товаров или услуг, может (2) ввести номер своего мобильного устройства на сайте удаленного продавца в качестве номера платежной карты. Сервер продавца формирует информацию платежа со всей необходимой информацией транзакции, содержащей профиль терминала точки продаж продавца, например номер основного счета и другую информацию, информацию управления риском, информацию обработки платежа, информацию о типе (типах) принимаемых карт, список кодов стран, в которых данному мобильному терминалу точки продаж разрешено осуществлять транзакции, список кодов стран, в которых данному мобильному терминалу точки продаж запрещено осуществлять транзакции, дату и время покупки, наименование продавца и сумму, а также номер пользовательского мобильного устройства и, возможно, другие элементы. Выставленный счет на оплату подписывается собственным секретным ключом продавца, который подписан доверенной третьей стороной, например банком, системой карточных платежей, удостоверяющим центром и т.п., и пересылается (3) в банк-эквайер, который проверяет подлинность и целостность данного счета. Если счет на оплату действителен, то УЦ подписывает его собственным секретным ключом и передает (4) в защищенную прикладную программу терминала точки продаж в пользовательском мобильном устройстве или в карте UICC/SIM в указанном мобильном устройстве.

Функция передачи данных может выполняться доверенным сервис-менеджером или другой доверенной третьей стороной. Для передачи данных может использоваться любой доступный протокол связи (например, передача мгновенных сообщений, SMS, USSD, TCP/IP или CSD), поддерживаемый используемой сетью, мобильным устройством и картой UICC, которая может находиться в данном мобильном устройстве.

Доверенная третья сторона, например УЦ или банк, может вести базу данных, связывающую указанный номер счета с номером мобильного устройства.

Терминал точки продаж принимает подписанный счет на оплату и проверяет целостность и подлинность данного счета с использованием находящегося в защищенной памяти данного терминала открытого ключа УЦ, доверенной третьей стороны или системы карточных платежей.

Терминал точки продаж предпочтительно определяет свое географическое местоположение с использованием, например, доступной в сети информации о том, в какой стране он находится, и сравнивает эту информацию о местоположении со списком кодов разрешенных и запрещенных стран. Если текущее географическое местоположение терминала точки продаж находится за пределами разрешенных местоположений или является запрещенным местоположением, то терминал точки продаж отменяет транзакцию, при этом могут оповещаться пользователь и банк.

Если информация платежа действительна, то терминал точки продаж использует информацию, содержащуюся в этой информации платежа, для своего конфигурирования с целью придания указанному терминалу возможности функционирования таким образом, как если бы это был терминал точки продаж, принадлежащий продавцу.

Информация платежа содержит сумму, подлежащую оплате, в виде неизменного числа, которое не может быть введено или иным образом модифицировано пользователем.

Пользователь может уведомляться о находящейся в процессе выполнения удаленной транзакции и у пользователя может запрашиваться разрешение на продолжение выполнения этой транзакции. Пользователь может отменить или разрешить транзакцию в том виде, в котором она сформирована, но не может изменить сумму, иные параметры или информацию, относящиеся к данной транзакции.

Терминал точки продаж отображает сумму, наименование или другой идентификатор продавца, и, возможно, другую информацию, относящуюся к данной транзакции, и запрашивает у пользователя одобрение транзакции. Если транзакция одобрена пользователем, то терминал точки продаж запрашивает представление платежной карты в считыватель карт. В случае множества карт или считывателей карт терминал точки продаж запрашивает у пользователя выбор подлежащей использованию карты и интерфейса считывателя карт.

Считыватель карт может быть встроен в терминал точки продаж/мобильное устройство или может быть внешним считывателем карт, соединенным с этим терминалом. Считыватель карт может быть контактным или бесконтактным.

При осуществлении (5) связи платежной карты со считывателем карт, встроенным или соединенным с мобильным устройством, с целью выполнения транзакции у пользователя может запрашиваться предоставление известной ему информации, например секретного кода PIN (Personal Identification Number персональный идентификационный номер), или иного средства аутентификации, например подписи, изображения, образца голоса, фотографии и т.д. Код PIN или иная информация аутентификации может вводиться, например, с использованием дисплея пользовательского интерфейса мобильного устройства, клавиатуры, камеры, средства распознавания голоса, средства распознавания символов, средства распознавания движений или средства распознавания отпечатка пальца.

Транзакция между платежной картой и терминалом точки продаж может быть, например, транзакцией стандарта EMV, бесконтактной платежной транзакцией, транзакцией со смарт-картой, транзакцией со встроенной платежной картой, транзакцией с кредитной или дебитной картой, транзакцией с использованием счета, например, у оператора сети, транзакцией с использованием предоплаченной или хранимой суммы или транзакцией с электронным кошельком.

Эта платежная карта может быть физически отдельной платежной картой или может находиться в той же карте UICC или в том же мобильном устройстве, что и терминал точки продаж. Платежная карта может находиться в мобильном кошельке, который находится в мобильном устройстве или в карте UICC/SIM. Платежная карта может находиться в той же интегральной схеме (ИС), что и терминал точки продаж, или в отдельной ИС. Одна или обе указанных ИС могут быть встроены в карту UICC/SIM или в мобильное устройство. ИС, содержащая платежную карту, может быть встроена в мобильное устройство, а ИС, содержащая терминал точки продаж, может быть встроена в карту UICC, и наоборот.

Картой UICC может быть карта SIM и/или защищенный элемент.

Если используется мобильный кошелек, содержащий более одной платежной карты, то пользователь может выбирать желаемую платежную карту.

Затем платежная транзакция передается обратно эквайеру платежей, который проверяет допустимость транзакции у эмитента карты (7-8) и подтверждает статус транзакции терминалам точки продаж и удаленному продавцу (9). Удаленный продавец может подтверждать статус транзакции покупателю (10). Если транзакция выполнена успешно, то денежные средства переводятся на счет продавца.

Если транзакция не одобрена, то пользователь может отменить транзакцию или повторить ее с использованием той же или другой платежной карты или того же или другого считывателя карт.

После обработки и завершения транзакции индивидуальная для продавца конфигурация и информация платежа необратимо удаляются.

Данные варианты осуществления дают возможность совершения защищенных удаленных покупок с использованием совместимого с NFC мобильного устройства и карты UICC в качестве терминала точки продаж как для продавца, так и для покупателя.

Указанным терминалом точки продаж может быть любой подключенный к сети терминал точки продаж.

Указанным узлом платежного сервиса также может быть программное приложение или аппаратная реализация в мобильном устройстве или в карте SIM. В этом случае для проведения защищенной финансовой транзакции, которой должен осуществляться перевод со счета покупателя на счет продавца, прикладная программа терминала точки продаж продавца в мобильном устройстве или в карте SIM может быть выполнена с возможностью передачи профиля собственного терминала в прикладную программу терминала точки продаж покупателя.

База данных адресов.

Прикладная программа терминала точки продаж, база данных конфигураций точек продаж или сертификат открытого ключа терминала точки продаж могут содержать базу данных с одним или более адресом строения или иным физическим адресом. Указанные адреса могут использоваться, например, в качестве адреса для выставления счета и/или адреса доставки при удаленной покупке товаров. Этот адрес может сочетаться с информацией, передаваемой в банк-эквайер и/или продавцу. Информация адреса может подписываться терминалом точки продаж с использованием своего секретного ключа для аутентификации и шифроваться с использованием открытого ключа продавца или банка-эквайера для защиты.

База данных адресов может содержать неизменные адреса, которые пользователь не может менять, и дополнительные адреса, которые пользователь может менять.

Указанные адреса могут быть помечены как адреса для различных целей, например "адрес доставки", "адрес для выставления счета", "домашний адрес", "рабочий адрес", "адрес терминала точки продаж". Если в данных, переданных в банк-эквайер и/или продавцу, содержится адрес, и этот адрес помечен как "адрес доставки", то продавец должен использовать указанный адрес в качестве адреса доставки товаров. Если адрес помечен как адрес для выставления счета, то продавец должен отправлять счет, относящийся к данной покупке, на указанный адрес.

Аспекты данного варианта (вариантов) осуществления также могут быть реализованы в виде про-

граммы, выполненной с возможностью использования с процессором для инициирования выполнения операций указанным процессором, или могут быть реализованы в виде аппаратуры на одном или более присоединенных или неприсоединенных устройствах.

Несмотря на то, что здесь проиллюстрированы и описаны предпочтительные формы и варианты осуществления настоящего изобретения, специалисту в данной области техники должно быть понятно, что возможны различные изменения без выхода за пределы представленной выше идеи изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система обработки удаленных транзакций, содержащая первое хранилище данных, содержащее профиль пользовательского устройства покупателя, относящийся к конфигурации пользовательского устройства покупателя и содержащий данные маршрутизации для маршрутизации связи с пользовательским устройством покупателя;

причем система выполнена с возможностью при приеме запроса платежа, в котором указано пользовательское устройство покупателя для выполнения транзакции с продавцом, получения профиля конфигурации платежного терминала продавца и получения из первого хранилища данных профиля конфигурации пользовательского устройства покупателя, соответствующего указанному пользовательскому устройству покупателя,

и с возможностью передачи данных о конфигурации платежного терминала продавца, используемого в точке продаж, в пользовательское устройство покупателя на основе данных маршрутизации,

при этом пользовательское устройство покупателя выполнено с возможностью использования данных о конфигурации платежного терминала продавца для обеспечения возможности использования пользовательского устройства покупателя в качестве платежного терминала продавца для выполнения транзакции с продавцом,

а данные о конфигурации платежного терминала продавца включают данные обработки платежа, чтобы задать пользовательскому устройству покупателя конфигурацию, обеспечивающую передачу данных об осуществлении платежа, произведенного на пользовательском устройстве покупателя, продавцу.

2. Система по п.1, отличающаяся тем, что профиль пользовательского устройства покупателя содержит открытый ключ из криптографической пары ключей пользовательского устройства покупателя, а система обработки удаленных транзакций выполнена с возможностью шифрования передаваемых данных о конфигурации платежного терминала продавца с использованием открытого ключа.

3. Система по п.1, отличающаяся тем, что маршрутам в данных маршрутизации назначены ранги, а система обработки удаленных транзакций выполнена с возможностью идентификации маршрута для достижения пользовательского устройства покупателя в зависимости от указанных рангов.

4. Система по п.1 или 3, отличающаяся тем, что маршруты включают маршруты для осуществления связи с пользовательским устройством покупателя через различные каналы.

5. Система по п.4, отличающаяся тем, что каналы выбраны из множества, содержащего SMS, мгновенные сообщения, связь с заранее определенным адресом в сети передачи данных или вызов для передачи данных по сети связи.

6. Система по любому из предшествующих пунктов, отличающаяся тем, что дополнительно содержит второе хранилище данных, содержащее профиль конфигурации каждого платежного терминала продавца из множества платежных терминалов продавцов, при этом указанная система выполнена с возможностью получения профиля конфигурации платежного терминала продавца из второго хранилища данных.

7. Система по любому из предшествующих пунктов, отличающаяся тем, что второе хранилище данных содержит сертификат платежного терминала продавца, относящийся к соответствующему продавцу и содержащий профиль конфигурации платежного терминала продавца.

8. Система по любому из предшествующих пунктов, отличающаяся тем, что первое хранилище данных содержит сертификат пользовательского устройства покупателя, относящийся к соответствующему пользовательскому устройству покупателя и содержащий открытый ключ пользовательского устройства покупателя.

9. Система по любому из предшествующих пунктов, отличающаяся тем, что первое и второе хранилища данных являются одним и тем же хранилищем данных.

10. Система по любому из предшествующих пунктов, отличающаяся тем, что первое хранилище данных содержит профиль пользовательского устройства покупателя для каждого пользовательского устройства покупателя из множества пользовательских устройств покупателя.

11. Система по п.10, отличающаяся тем, что первое хранилище данных является удаленным по отношению к пользовательскому устройству покупателя.

12. Система по любому из пп.1-9, отличающаяся тем, что первое хранилище данных является локальным по отношению к пользовательскому устройству покупателя.

13. Система по любому из предшествующих пунктов, отличающаяся тем, что дополнительно содержит веб-сайт продавца, содержащий платежный пользовательский интерфейс, реализованный с воз-

можностью приема от пользователя идентификатора, указывающего профиль пользовательского устройства покупателя, которое должно использоваться для платежа, при этом система выполнена с возможностью получения профиля пользовательского устройства покупателя в зависимости от указанного идентификатора.

14. Система по любому из предшествующих пунктов, отличающаяся тем, что дополнительно содержит систему обработки платежей, выполненную с возможностью приема запросов платежа для каждого продавца из множества продавцов.

15. Система по п.14, отличающаяся тем, что система обработки платежей выполнена с возможностью приема профиля конфигурации платежного терминала продавца от продавца при приеме запроса платежа.

16. Система по любому из предшествующих пунктов, отличающаяся тем, что дополнительно содержит пользовательское устройство покупателя, которое содержит прикладную программу платежного терминала продавца и считыватель платежных карт, при этом пользовательское устройство покупателя выполнено с возможностью приема конфигурации платежного терминала продавца для осуществления транзакции с продавцом, с возможностью конфигурирования прикладной программы платежного терминала продавца в зависимости от указанной конфигурации платежного терминала продавца и с возможностью считывания платежной карты посредством считывателя платежных карт для выполнения платежа по данной транзакции посредством прикладной программы платежного терминала продавца.

17. Система по п.16, отличающаяся тем, что пользовательское устройство покупателя содержит защищенный модуль, в котором выполняется прикладная программа платежного терминала продавца, при этом защищенный модуль выбран из множества, включающего модуль идентификации абонента (SIM), универсальную карту с интегральной схемой (UICC) или встроенный защищенный элемент (ESE), доверенную среду исполнения (TEE) или защищенную среду.

18. Система по п.17, отличающаяся тем, что защищенный модуль вставлен, вмонтирован или встроен в пользовательское устройство покупателя.

19. Способ обработки удаленных транзакций, реализуемый в системе обработки удаленных транзакций по независимому п.1, включающий следующие операции:

прием запроса платежа системой обработки удаленных транзакций с указанием пользовательского устройства покупателя для выполнения транзакции с продавцом;

получение системой обработки удаленных транзакций профиля конфигурации платежного терминала продавца;

получение системой обработки удаленных транзакций из первого хранилища данных профиля конфигурации пользовательского устройства покупателя, соответствующего указанному пользовательскому устройству покупателя, содержащего данные маршрутизации для маршрутизации связи с пользовательским устройством покупателя; и

передачу системой обработки удаленных транзакций данных о конфигурации платежного терминала продавца в пользовательское устройство покупателя на основе данных маршрутизации;

использование пользовательским устройством покупателя данных о конфигурации платежного терминала продавца для обеспечения возможности использования пользовательского устройства покупателя в качестве платежного терминала продавца для выполнения транзакции с продавцом,

при этом данные о конфигурации платежного терминала продавца включают данные обработки платежа, чтобы задать пользовательскому устройству покупателя конфигурацию, обеспечивающую передачу данных об осуществлении платежа, произведенного на пользовательском устройстве покупателя, продавцу.

20. Способ по п.19, отличающийся тем, что дополнительно включает

связывание криптографического сертификата, содержащего открытый ключ из пары открытого и секретного ключей, с профилем пользовательского устройства покупателя;

шифрование по меньшей мере части данных о конфигурации платежного терминала продавца с использованием открытого ключа и

расшифровку зашифрованных данных о конфигурации платежного терминала продавца в пользовательском устройстве покупателя с использованием секретного ключа.

21. Способ по п.20, отличающийся тем, что дополнительно включает сохранение криптографического сертификата в хранилище данных, при этом шаг получения профиля пользовательского устройства покупателя включает получение указанного сертификата.

22. Способ по любому из пп.19-21, отличающийся тем, что шаг приема запроса платежа включает прием информации о транзакции, а шаг передачи данных о конфигурации платежного терминала продавца включает формирование данных о конфигурации платежного терминала продавца на основе информации о транзакции и профиля конфигурации платежного терминала продавца.

23. Способ по п.22, отличающийся тем, что шаг формирования данных о конфигурации платежного терминала продавца включает операцию подписания данных о конфигурации платежного терминала продавца с использованием секретного ключа из криптографической пары секретного и открытого ключей.

24. Способ по любому из пп.19-23, отличающийся тем, что дополнительно включает выполнение в пользовательском устройстве покупателя следующих шагов:

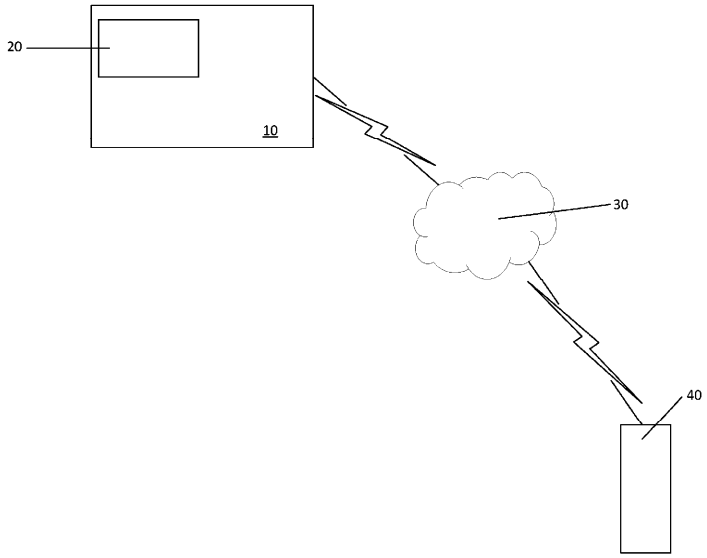
выполнение транзакции карточного платежа с использованием платежной карты в пользовательском устройстве покупателя во взаимодействии с платежным терминалом продавца;

подписание в платежном терминале продавца данных транзакции платежа;

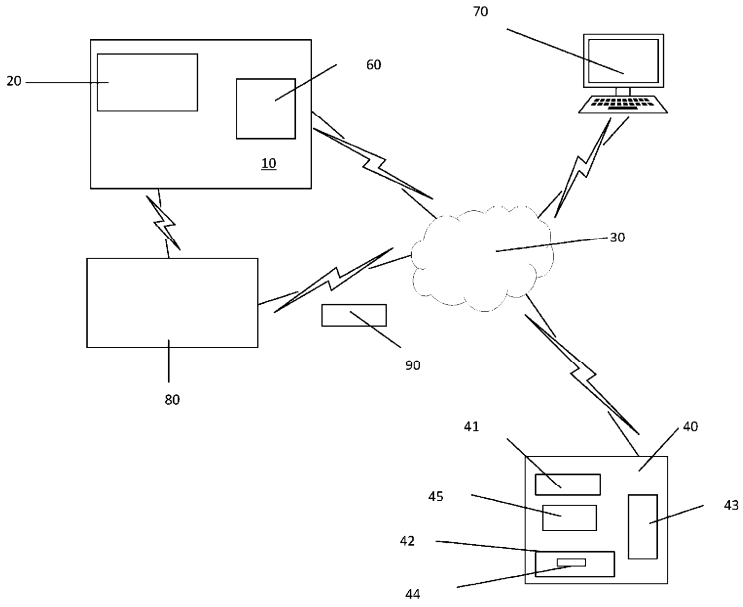
шифрование в платежном терминале продавца подписанных данных транзакции платежа;

передачу платежным терминалом продавца зашифрованных и подписанных данных транзакции платежа в узел платежного сервиса и

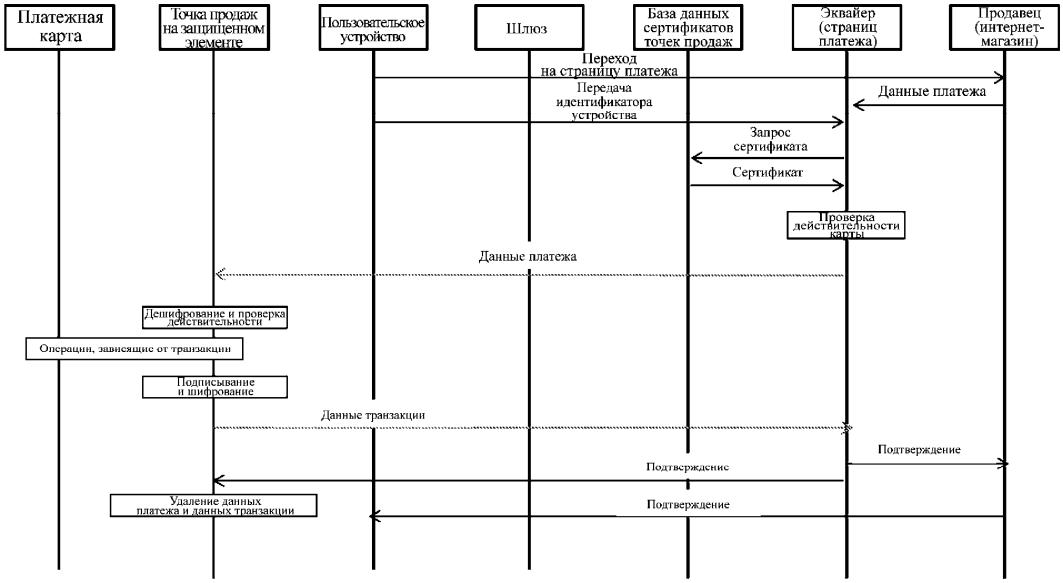
удаление платежным терминалом продавца указанной информации данных транзакции платежа из собственной памяти.



Фиг. 1



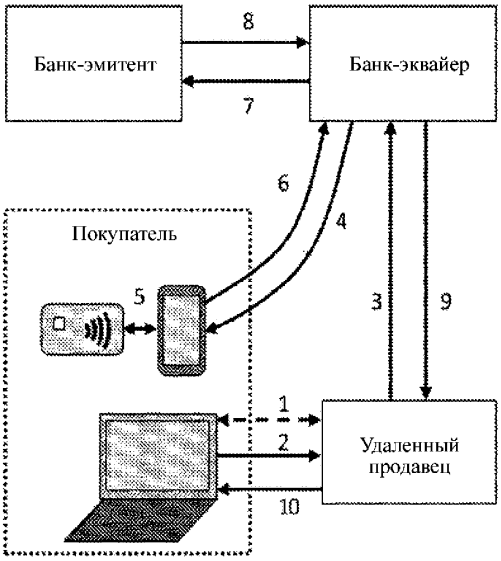
Фиг. 2


Платежная карта
Точка продаж на защищенном элементе
Пользовательское устройство
Шлюз
База данных сертификатов точек продаж
Эквайер (страниц платежа)
Продавец (интернет-магазин)
Переход на страницу платежа
Данные платежа
Передача идентификатора устройства
Запрос сертификата
Сертификат
Проверка действительности карты
Данные платежа
Дешифрование и проверка действительности
Операции, зависящие от транзакции
Подписывание и шифрование
Данные транзакции
Подтверждение
Подтверждение
Удаление данных платежа и данных транзакции
Подтверждение

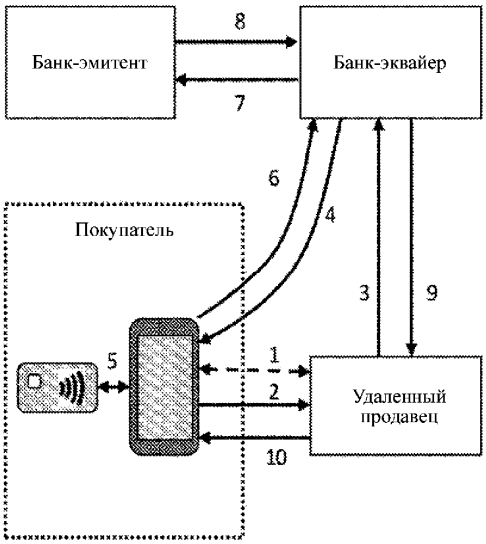
Фиг. 3


Начало
Подписывание информации платежа секретным ключом продавца
Сообщение подписанной информации платежа и сертификата открытого ключа продавца в пользовательское устройство, работающее в качестве терминала точки продаж
Проверка пользовательским устройством действительности сертификата открытого ключа с использованием сертификата открытого ключа удостоверяющего центра
Сертификат действителен?
Нет
Да
Проверка действительности информации платежа с использованием сертификата открытого ключа продавца
Информация платежа действительна?
Нет
Да
Конфигурирование терминала точки продаж в пользовательском устройстве в соответствии с информацией платежа
Представление инструкций платежа пользователю посредством пользовательского устройства
Пользователь согласен с платежом?
Да
Обработка платежа
Нет
Удаление профиля из терминала точки продаж
Конец

Фиг. 4



Фиг. 5



Фиг. 6

Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2