

(19)



**Евразийское
патентное
ведомство**

(11) **035549**(13) **B1**(12) **ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ**

(45) Дата публикации и выдачи патента
2020.07.06

(21) Номер заявки
201892669

(22) Дата подачи заявки
2017.05.12

(51) Int. Cl. **G06Q 20/08** (2012.01)
G06Q 20/10 (2012.01)
G06Q 20/22 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/38 (2012.01)
G06F 17/30 (2006.01)

(54) СИСТЕМА ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ И СПОСОБ ИХ СОВЕРШЕНИЯ

(31) **201621021488**

(32) **2016.06.22**

(33) **IN**

(43) **2019.04.30**

(86) **PCT/IB2017/052793**

(87) **WO 2017/221085 2017.12.28**

(71)(73) Заявитель и патентовладелец:
**НЭШИОНАЛ ПЕЙМЕНТС
КОРПОРАЙШН ОФ ИНДИА (IN)**

(72) Изобретатель:
**Асбе Дилип, Раэндран Нараянан,
Палагири Сатеш, Шарма Анобхав
(IN)**

(74) Представитель:
Зуйков С.А. (RU)

(56) "Unified Payment Interface: API and Technology Specifications - Version 1.0" (NPCI), 15 April 2015 (15-04-2015), URL: http://npci.org.in/documents/Technical_Specifications.pdf, (retrieved on 08-06-2017), Chapters 1-4, Pages 5-32; Figures 4.1, 4.2

IN-A-MUM-2015-02256

(57) Изобретение описывает систему электронных платежей и способ их совершения. Изобретение относится к области систем электронных платежей. Система электронных платежей упрощает отправку и прием денег более простым способом с использованием пользовательских устройств. Она предоставляет собой унифицированный платежный интерфейс (UPI) и предоставляет возможность пользователям оплачивать и получать/инкассировать платежи со счетов заинтересованных физических/юридических лиц. Система по изобретению предоставляет возможность совершения платежных транзакций между плательщиком и получателем платежа без необходимости обязательного предоставления банковской информации и реквизитов банковского счета друг друга. Она устраняет риск хранения реквизитов счета покупателя и может использоваться покупателями, которые не имеют кредитной/дебетовой карты. Она обеспечивает конфиденциальность платежной транзакции и упрощает установление множества утилит, оплату наличными при доставке, при разделении/совместном использовании счетов, при оплате/переводе денег продавцу. Система электронных платежей по изобретению работает через различные интерфейсы, посредством которой запросы на платеж могут быть сгенерированы в Интернет-интерфейсе и авторизованы в мобильном интерфейсе (инструмент приложения).

B1**035549****035549****B1**

Область техники, к которой относится изобретение

Изобретение относится к системам электронных платежей.

Термины и определения

Выражение "зарегистрированный пользователь", используемое в дальнейшем в описании настоящего изобретения, относится к лицу, использующему систему электронных платежей (EPS) по настоящему изобретению для совершения транзакций в системе электронных платежей. Зарегистрированным пользователем может быть плательщик, т.е. лицо, которое хочет отправить/заплатить деньги, используя EPS, или им может быть получатель платежа, т.е. лицо, которое получает/инкассирует деньги, используя EPS.

Выражение "пользовательское устройство", используемое в дальнейшем в описании настоящего изобретения, относится к устройству, используемому зарегистрированным пользователем, при этом пользовательское устройство включает, но этим не ограничивается, мобильный телефон, лэптоп, планшет, iPad, КПК, ноутбук, нетбук, интеллектуальное устройство, смартфон, персональный компьютер, портативное устройство и тому подобное.

Выражение "платежные транзакции", используемое в дальнейшем в описании настоящего изобретения, относится как к финансовым, так и к нефинансовым транзакциям. Финансовые транзакции содержат запросы на инкассацию/pull-запросы, запросы на оплату/push-запросы и коммерческие платежи. Нефинансовые транзакции включают, но этим не ограничиваются, регистрацию мобильного банкинга, генерацию одноразового пароля (OTP), проверку баланса, установку или изменение PIN-кода, регистрацию жалобы и проверку статуса транзакции.

Выражение "Система оператора платежного сервиса (PSPS)", используемое в дальнейшем в описании настоящего изобретения, относится к Банку, Платежному банку или к любому другому юридическому лицу, которое регулируется централизованным образом или государством, которому разрешено привлекать покупателей и предоставлять платежные сервисы (кредитовые/дебетовые) покупателям (физическим или юридическим лицам). PSPS предоставляет инструменты соответствующих приложений, к которым зарегистрированные пользователи могут получить доступ на своих пользовательских устройствах для выполнения push- или pull-платежей. PSPS предоставляет инструмент для электронной обработки финансовых и нефинансовых транзакций.

Выражение "отправитель", используемое в дальнейшем в описании настоящего изобретения, относится к зарегистрированному пользователю, который отправляет запрос на оплату/push-запрос или запрос на инкассацию денег/pull-запрос, используя пользовательское устройство по настоящему изобретению. Отправителем может быть плательщик или получатель платежа.

Выражение "получатель", используемое в дальнейшем в описании настоящего изобретения, относится к зарегистрированному пользователю, который получает запрос на пользовательском устройстве на инкассацию денег/pull-запрос или запрос на оплату денег/push-запрос, используя пользовательское устройство по настоящему изобретению. Получателем может быть получатель платежа или плательщик.

Выражение "уникальный идентификатор (ID)" или "виртуальный платежный адрес (VPA)", используемое в дальнейшем в описании настоящего изобретения, относится к уникальному идентификатору, связанному с зарегистрированным пользователем. Уникальный ID или Виртуальный платежный адрес (VPA) используется для совершения платежных транзакций. Он может быть создан зарегистрированным пользователем для совершения платежной транзакции(ий).

Выражение "унифицированный платежный интерфейс (UPI)", используемое в дальнейшем в описании настоящего изобретения, относится к интерфейсной системе, которая предоставляет интерфейс между системами PSPS для совершения финансовых и нефинансовых платежных транзакций, включая платежные транзакции и расчетные платежи.

Выражение "Приложение оператора платежного сервиса (PSPA)", используемое в дальнейшем в описании настоящего изобретения, относится к инструменту приложения, предоставляемому каждой PSPS. Инструмент PSPA может быть предоставлен на Интернет-портале или в магазине игр и/или в мобильном Интернете, или с помощью других средств для взаимодействия с PSPS посредством UPI.

Выражение "информационные данные о пользователе", используемое в дальнейшем в описании настоящего изобретения, относится к данным, относящимся к зарегистрированному пользователю, включая VPA зарегистрированного пользователя, данные учетной записи и другие нефинансовые данные. Информационные данные о пользователе используются для аутентификации зарегистрированного пользователя.

Эти термины и определения дополняют термины и определения, существующие в данной области техники.

Предпосылки создания изобретения

В последние годы финансовые транзакции все чаще совершаются с использованием портативных устройств, т.е. традиционных мобильных телефонов и смартфонов. В настоящее время доступны различные способы оплаты с использованием портативных устройств. Эти способы оплаты требуют знания номера счета получателя платежа и дополнительных данных, относящихся к банку получателя платежа. В случае онлайн-платежей плательщику необходимо зайти на Интернет-портал своего банка с помощью Интернет-банкинга или мобильного банкинга для совершения финансовых транзакций. На сегодняшний

день многие пользователи все еще нечасто пользуются финансовыми транзакциями онлайн/электронными транзакциями, так как банковские Интернет-порталы для Интернет-банкинга или мобильного банкинга - неудобны или сложны в использовании; и для ввода данных и авторизации требуется длительное время.

В некоторых случаях номер мобильного телефона получателя платежа используется для выполнения платежа. Однако при таком способе крайне важно для плательщика знать банковские реквизиты получателя платежа и/или номер мобильного телефона, так как мобильный банкинг привязан к номеру SIM-карты. При совершении всех таких транзакций платеж направляется плательщиком получателю платежа. Получатель платежа зависит исключительно от плательщика, совершающего транзакции, а плательщик зависит от Интернет-портала своего банка, реализующего платежный сервис. Некоторые пользователи склонны менять свои номера мобильных телефонов, и в таких случаях плательщику сложно отследить эти изменения. Кроме того, в некоторых случаях плательщик и получатель платежа могут не захотеть раскрывать свои банковские реквизиты и личные данные друг другу.

Соответственно, существует необходимость в ограничении вышеупомянутых недостатков и в том, чтобы была предложена эффективная, простая и удобная в использовании система и способ совершения транзакций в системе электронных платежей.

Цели изобретения

Далее представлены некоторые из целей настоящего изобретения, которым удовлетворяет по меньшей мере один вариант его осуществления, описанный в настоящем документе.

Именно устранение по меньшей мере одной проблемы известного уровня техники или, по меньшей мере, предложение полезной альтернативы является целью настоящего изобретения.

Целью настоящего изобретения является предложение системы электронных платежей, которая проста в использовании.

Другой целью настоящего изобретения является предложение системы электронных платежей, имеющей унифицированный платежный интерфейс (UPI).

Еще одной целью настоящего изобретения является предложение системы электронных платежей, которая предоставляет возможность пользователям совершать pull-платежи/инкассирует платежи со счетов заинтересованных физически/юридических лиц после того, как запрашиваемое юридическое лицо авторизует такие платежи.

Еще одной целью настоящего изобретения является упрощение системы электронных платежей как для плательщиков, так и для получателей платежей путем сокращения этапов авторизации и повышения функций безопасности.

Еще одной целью настоящего изобретения является предложение системы электронных платежей, которая предоставляет возможность выполнять платежные транзакции между плательщиком и получателем платежа без необходимости обязательного предоставления банковской информации и реквизитов банковского счета друг друга.

Кроме того, целью настоящего изобретения является предложение системы электронных платежей, которая предоставляет возможность пользователю отправлять и получать деньги с помощью виртуального платежного адреса.

Еще одной целью настоящего изобретения является предложение системы электронных платежей, которая устраняет зависимость пользователя от Интернет-портала своего банка или мобильного приложения для Интернет-банкинга или мобильного банкинга, и позволяет пользователю использовать Интернет-портал другого банка и/или мобильные приложения для совершения платежных транзакций, отличные от его банковского счета.

Другие цели и преимущества настоящего изобретения будут более очевидны из нижеследующего описания, которое никоим образом не ограничивает объем настоящего изобретения.

Краткое изложение сущности изобретения

Система электронных платежей (EPS) и способ их совершения предусмотрены для упрощения совершения платежных транзакций между множеством пользователей. Система содержит оперативное запоминающее устройство, операционный процессор, множество Систем операторов платежного сервиса (PSPS), выполненных с возможностью регистрации пользователей, и выполненных с дополнительной возможностью регистрации их в EPS, множество пользовательских устройств, инструменты Приложений операторов платежного сервиса (PSPAs) и Унифицированный платежный интерфейс (UPI). Оперативное запоминающее устройство хранит набор предварительно заданных правил действий, которые используются операционным процессором для получения набора команд управления работой системы. Каждая PSPS содержит локальное запоминающее устройство, которое хранит информационные данные о пользователе, относящиеся к пользователям, зарегистрированным в PSPS по меньшей мере одну поисковую таблицу, которая упрощает сопоставление данных, введенных покупателем, информационных данных о пользователе и о зарегистрированном пользователе, и PSPS-сервер. Каждое пользовательское устройство из множества пользовательских устройств связано с одним из зарегистрированных пользователей и зарегистрировано в качестве части информационных данных о пользователе. Каждый инструмент PSPA связан и размещен на своем ресурсе PSPS-сервером системы PSPS, зарегистрированной в EPS, и содержит

элементы, которые загружаются и хранятся в пользовательском устройстве зарегистрированного пользователя независимо от того, зарегистрирован ли зарегистрированный пользователь в PSPS, связанной с инструментом PSPA, или нет. Каждый инструмент PSPS упрощает генерацию и получение сигналов по данным о транзакции, относящихся к запросам на платеж от зарегистрированных пользователей, и к кредитовым и/или дебетовым счетам зарегистрированных пользователей на основании этих запросов. Загружаемые элементы каждого инструмента PSPA содержат модуль регистрации и модуль создания виртуального платежного адреса (VPA). Модуль регистрации разрешает регистрацию пользовательского устройства в зарегистрированной PSPS, связанной с инструментом PSPA во взаимно-однозначном соответствии. Модуль создания VPA позволяет зарегистрированному пользователю создать уникальный VPA, который включает идентификацию PSPS, в которой зарегистрирован зарегистрированный пользователь, и в дальнейшем предоставляет возможность пользовательскому устройству отправить уникальный VPA на локальное запоминающее устройство системы PSPS, в которой зарегистрирован пользователь, в качестве части информационных данных о пользователе от зарегистрированного пользователя. UPI упрощает регистрацию PSPS в EPS и в дальнейшем упрощает управляемое перемещение сигналов по данным о транзакции, выборочно, между системами PSPS для осуществления платежа от одного зарегистрированного пользователя к другому зарегистрированному пользователю в одинаковых или разных системах PSPS. UPI содержит модуль расчетов, который взаимодействует с множеством систем PSPS для периодического сопоставления кредитовых и дебетовых транзакций и генерирования инструкций по чистому кредиту и дебету между зарегистрированными системами PSPS.

Краткое описание сопроводительного чертежа

Система электронных платежей и способ их совершения по изобретению теперь будут описаны с помощью сопроводительного чертежа, при этом

на фиг. 1 представлена блок-схема системы электронных платежей (EPS) в соответствии с одним вариантом осуществления настоящего изобретения;

на фиг. 2А - схема, показывающая поток транзакции по типу клиент-клиент с использованием EPS в соответствии с одним вариантом осуществления настоящего изобретения, представленном на фиг. 1;

на фиг. 2В - схема, показывающая другой поток транзакции по типу клиент-клиент, с использованием EPS, в соответствии с одним вариантом осуществления изобретения, представленном на фиг. 1;

на фиг. 3 - диаграмма процесса потока платежной транзакции, совершаемого в случае инкассируемого платежа, совершаемого с помощью EPS, как показано на фиг. 2А;

на фиг. 4 - диаграмма процесса, показывающая поток платежной транзакции, совершаемый в случае прямого платежа, совершаемого с помощью EPS, как показано на фиг. 2В;

на фиг. 5 - диаграмма потока, показывающая платежную транзакцию между водителем такси и его пассажиром, совершаемую с помощью EPS, как показано на фиг. 1;

на фиг. 6 - диаграмма потока, показывающая платежную транзакцию по переводу платежа, совершаемую с помощью EPS, как показано на фиг. 1;

на фиг. 7 - диаграмма потока, показывающая трехстороннюю коммерческую транзакцию, совершаемую между покупателем и продавцом, у которых имеется одинаковая PSPS, в соответствии с одним вариантом осуществления настоящего изобретения, представленном на фиг. 1; и

Список позиций и их обозначений, используемых в описании и на чертежах

Позиция	Обозначение
1000	Система электронных платежей (EPS)
100, 500, 600, 700	Унифицированный платежный интерфейс (UPI)
100A	Модуль расчетов
100b	Приемник
100c	Анализатор
100d	Извлекатель идентификатора
100e	Передатчик
1002a	Оперативное запоминающее устройство
1002b	Операционный процессор
1004	Система оператора платежного сервиса (PSPS)
1004a	Локальное запоминающее устройство
1004b	По меньшей мере, одна поисковая таблица
1004c	PSPS-сервер
1006	Пользовательское устройство
1008	Инструмент Приложения оператора платежного сервиса (PSPA)
1008a	Модуль регистрации
1008b	Модуль создания виртуального платежного адреса (VPA)
102, 502, 702	Пользовательское устройство Получателя платежа
104, 504, 604	Пользовательское устройство Плательщика
106, 506, 606	PSPS Получателя платежа
108, 508, 608	PSPS Плательщика
110, 510, 610, 706	Банк-ремитент/ Эмитент/ банк Плательщика
112, 512, 612, 708	Банк-бенефициар/ Эквайер/ банк Получателя платежа
704	PSPS (общие PSPS) Продавца/Покупателя
710	Покупатель

Подробное описание вариантов осуществления изобретения

Теперь будет приведено описание настоящего изобретения со ссылкой на сопроводительный чертеж, который представляет, но не ограничивает объем притязаний и сферу применения настоящего изобретения. Данное описание приведено исключительно в качестве примера и для наглядности.

Несколько лет назад держателям банковских счетов разрешалось использовать свои дебетовые/пластиковые карты для совершения денежных транзакций только в авторизованных банкоматах, принадлежащих банку держателя счета. С увеличением потребностей пользователей, клиентов и покупателей банковских услуг была разработана новая модель, которая предусматривала расширение доступа к банкоматам, предоставляя возможность держателям банковских счетов использовать банкоматы, принадлежащие любым банкам. В настоящее время любое лицо может использовать любой банкомат по всему миру, независимо от своего конкретного банка. Это упрощает установление универсальной взаимной высокой мобильности между банкоматами и дебетовыми/пластиковыми картами в различных сетях, выполняющих обработку транзакций и расчет средств между участниками транзакции.

В настоящем изобретении рассматривается взаимодействие банковских мобильных приложений и/или банковских Интернет-порталов при совершении платежных транзакций. Используя систему по настоящему изобретению, пользователи и/или покупатели банковских услуг не ограничены использованием Интернет-порталов и/или мобильных Интернет-сайтов банков, в которых они держат свой счет(счета). Вместе с тем пользователи (как плательщик, так и получатель платежа) и/или покупатели могут выбрать Интернет-портал или мобильный Интернет-сайт любого банка для совершения своих пла-

тежных транзакций, не зная реквизитов банковского счета другого пользователя/лица. Пользователям (плательщику или получателю платежа) необходимо знать только уникальный ID или виртуальный платежный адрес (VPA) для совершения транзакций в системе финансовых/электронных платежей.

Как показано на сопроводительном чертеже, на фиг. 1 представлена блок-схема системы электронных платежей (1000) (именуемой в дальнейшем EPS), которая упрощает совершение платежных транзакций между множеством пользователей. Платежные транзакции включают и финансовые, и нефинансовые транзакции, при этом финансовые транзакции содержат запросы на инкассацию/pull-запросы, запросы на оплату/push-запросы и коммерческие платежи, а нефинансовые транзакции содержат регистрацию мобильного банкинга, генерацию одноразового пароля (OTP), установку или изменение PIN-кода, проверку статуса транзакции, регистрацию жалобы и тому подобное.

EPS (1000) содержит оперативное запоминающее устройство (1002a), операционный процессор (1002b), множество Систем операторов платежного сервиса (PSPS), множество пользовательских устройств, инструменты Приложения оператора платежного сервиса (PSPA), Унифицированный платежный интерфейс (UPI) (100).

Оперативное запоминающее устройство (1002a) выполнено с возможностью хранения набора предварительно заданных правил действий. Оперативное запоминающее устройство (1002a) может включать любой машиночитаемый носитель, известный в данной области техники, в том числе, например, энергозависимое запоминающее устройство, такое как статическое запоминающее устройство с произвольной выборкой (SRAM) и динамическое запоминающее устройство с произвольной выборкой (DRAM), и/или энергонезависимое запоминающее устройство, такое как постоянное запоминающее устройство (ROM), электрически стираемое программируемое ROM, флэш-память, жесткие диски, оптические диски и ленты для магнитной записи или облачную систему хранения (облачное хранение). В одном варианте осуществления настоящего изобретения оперативное запоминающее устройство (1002a) выполнено с возможностью хранения предварительно заданных правил действий, относящихся к транзакциям в системе электронных платежей, к передаче и приему запросов на платеж и тому подобное.

Операционный процессор (1002b) выполнен с возможностью взаимодействия с оперативным запоминающим устройством (1002a) для приема и обработки предварительно заданных правил действий для получения набора команд управления работой системы. Операционный процессор (1002b) может быть реализован по меньшей мере как один микропроцессор, микрокомпьютер, микроконтроллер, цифровой сигнальный процессор, центральный вычислительный блок, конечная машина, логическая схема и/или любое устройство, которое обрабатывает сигналы на основании операционных инструкций. Помимо других функциональных возможностей, операционный процессор (1002b) выполнен с возможностью вызова и выполнения предварительно заданного набора правил действий, хранящегося в оперативном запоминающем устройстве (1002a), для управления модулями EPS 1000.

Множество Систем операторов платежного сервиса (PSPS) регистрируются в EPS (1000), и они выполнены с возможностью регистрации пользователей. Каждая PSPS (1004) содержит локальное запоминающее устройство (1004a) по меньшей мере одну поисковую таблицу (1004b) и PSPS-сервер (1004c). Локальное запоминающее устройство (1004a) хранит информационные данные о пользователе, относящиеся к пользователям, зарегистрированным в PSPS (1004). В одном варианте осуществления настоящего изобретения, данные о пользователе включают виртуальный платежный адрес (VPA), данные учетной записи и другие нефинансовые данные зарегистрированного пользователя для упрощения аутентификации зарегистрированного пользователя. По меньшей мере одна поисковая таблица (1004b) упрощает сопоставление данных, введенных покупателем, информационных данных о пользователе и о зарегистрированном пользователе.

Каждое пользовательское устройство (1006) из множества пользовательских устройств связано с одним из зарегистрированных пользователей и регистрируется в качестве части информационных данных о пользователе. Каждый из зарегистрированных пользователей использует зарегистрированное пользовательское устройство для генерирования сигналов по данным о транзакции, относящихся к запросам на платежи посредством инструмента PSPA.

Каждый инструмент PSPA (1008), из инструментов PSPA, связан и размещен на своем ресурсе PSPS-сервером (1004c) системы PSPS (1004), зарегистрированной в вышеупомянутой EPS (1000), и содержит элементы, которые загружаются и хранятся в пользовательском устройстве (1006) зарегистрированного пользователя, независимо от того, зарегистрирован ли зарегистрированный пользователь в PSPS, связанной с инструментом PSPA (1008), или нет. Каждый инструмент PSPS (1008) упрощает генерацию и прием сигналов по данным о транзакции, относящихся к запросам на платеж, поступающим от вышеупомянутых зарегистрированных пользователей, и к кредитовым и/или дебетовым счетам зарегистрированных пользователей на основании этих запросов.

Загружаемые элементы каждого инструмента PSPA (1008) содержат модуль регистрации (1008a) и модуль создания виртуального платежного адреса (VPA) (1008b). Модуль регистрации (1008a) разрешает регистрацию пользовательского устройства (1006) в зарегистрированной PSPS (1004), связанной с инструментом PSPA (1008) во взаимнооднозначном соответствии. Модуль создания VPA (1008b) предоставляет возможность зарегистрированному пользователю создать уникальный VPA, который включает

идентификацию PSPS, в которой зарегистрирован зарегистрированный пользователь, и в дальнейшем предоставляет возможность пользовательскому устройству (100б) передать уникальный VPA на локальное запоминающее устройство (1004а) системы PSPS (1004), в которой зарегистрирован пользователь, в качестве части информационных данных о пользователе от зарегистрированного пользователя.

UPI (100) упрощает регистрацию PSPS (1004) в EPS (1000) и в дальнейшем упрощает управляемое перемещение сигналов по данным о транзакции, выборочно, между системами PSPS для осуществления платежа от одного зарегистрированного пользователя к другому зарегистрированному пользователю в одинаковых или разных системах PSPS. UPI (100) содержит модуль расчетов (100а), который взаимодействует с множеством систем PSPS для периодического сопоставления кредитовых и дебетовых транзакций, и генерирования инструкций по чистому кредиту и дебету между зарегистрированными системами PSPS. В одном варианте осуществления настоящего изобретения модуль расчетов (100а) представляет собой сервер расчетов.

Для того чтобы упростить управляемое перемещение данных о транзакции, UPI (100) дополнительно содержит приемник (100б), анализатор (100с), извлекатель (100д) и передатчик (100е). Приемник (100б) принимает сигналы по данным о транзакции, относящиеся к запросам на платеж, поступающие от зарегистрированных пользовательских устройств посредством любого из инструментов PSPA. Каждый запрос на платеж содержит VPA первого зарегистрированного пользователя, VPA второго зарегистрированного пользователя и сумму транзакции, таким образом, эти VPA включают информацию, относящуюся к системам PSPS, в которых зарегистрированы первый зарегистрированный пользователь и второй зарегистрированный пользователь. Анализатор (100с) анализирует сигналы по данным о транзакции для получения проанализированных сигналов. Затем информация, относящаяся к PSPS первого зарегистрированного пользователя и к PSPS второго зарегистрированного пользователя, извлекается и идентифицируется из проанализированных сигналов с помощью извлекателя идентификатора (100д). Затем передатчик (100е) передает сигналы по данным о транзакции идентифицированным соответствующим PSPS, для того, чтобы упростить списание кредитового платежа со счета первого зарегистрированного пользователя на счет второго зарегистрированного пользователя или зачисление дебетового платежа на счет первого зарегистрированного пользователя со счета второго зарегистрированного пользователя, выборочно, на основании содержимого данных проанализированных сигналов.

На фиг. 2А и 2В сопроводительного чертежа представлены схемы, показывающие потоки транзакции по типу клиент-клиент, с использованием UPI (100) для платежных транзакций. UPI (100) представляет собой интерфейс, имеющий множество серверов.

В одном варианте осуществления настоящего изобретения UPI (100) имеет сервер транзакций, сервер авторизации, UPI-сервер и сервер расчетов. Сервер транзакций обрабатывает сигналы по данным о транзакции, сервер авторизации авторизует зарегистрированных пользователей, а UPI-сервер обрабатывает сохраненный набор правил действий для идентификации зарегистрированных систем PSPS. UPI (100) взаимодействует с банками на основании инструкций/запросов от PSPS, созданных с помощью инструментов PSPA. UPI (100) совершает обработку транзакций и расчетные платежи. В одном варианте осуществления настоящего изобретения обработка транзакций выполняется с помощью сервера транзакций. Расчетные платежи между банками и системами PSPS в конце дня осуществляются с использованием сервера расчетов. В одном варианте осуществления настоящего изобретения, PSPS-сервер размещает на своем ресурсе инструмент PSPA, который может использоваться зарегистрированными пользователями для передачи запросов на платеж. Запрос на платеж может представлять собой запрос на оплату/push-запрос или запрос на инкассацию/pull-запрос.

Запрос на pull-платеж представляет собой запрос, по которому физическому/юридическому лицу необходимо инкассировать платеж от другого физического/юридического лица. Запрос на push-платеж представляет собой запрос, по которому физическому/юридическому лицу необходимо заплатить определенную сумму другому физическому/юридическому лицу. В одном варианте осуществления настоящего изобретения этапы, предоставляющие возможность пользователю совершить push-платеж или pull-платеж, включают следующее:

- а) регистрация в PSPS;
- б) регистрация в мобильном банкинге и генерирование PIN-кода UPI для транзакций (если к этому моменту он не был зарегистрирован);
- в) загрузка инструмента PSPA, предоставленного любым PSPS, на пользовательское устройство, и создание профиля зарегистрированного пользователя путем предоставления данных учетной записи с помощью пароля/PIN-кода логина с использованием инструмента PSPA;
- д) используя систему по настоящему изобретению, создание VPA в качестве уникального ID с использованием инструмента PSPA, в результате чего VPA связан с любыми реквизитами банковского счета(счетов) пользователя; и
- е) передача push-запросов или pull-запросов/данных о транзакции посредством инструмента PSPA.

PSPS представляет собой банк, который предоставляет инструмент PSPA и который может быть зарегистрирован в EPS (1000) для того, чтобы использовать UPI (100). На вышеупомянутом этапе "а" "регистрации в PSPS" пользователи регистрируются в банке, по своему выбору, путем открытия счета в

банке. Если пользователь уже имеет счет в банке, он может зарегистрироваться в мобильном банкинге, предоставив необходимые данные, включая данные о своем пользовательском устройстве для того, чтобы зарегистрировать пользовательское устройство. После завершения регистрации пользователь может загрузить инструменты PSPA, как указано на этапе "с" выше. Пользователь (например, плательщик или получатель платежа) использует свое пользовательское устройство для доступа к инструменту PSPA по своему выбору, независимо от того, держит ли он счет в банке, который предоставляет инструмент PSPA. На этапе "d" пользователь должен создать VPA. Изображение создания VPA представлено на фиг. 8А. Поскольку пользователь зарегистрирован в своем банке, он предоставляет те же данные для того, чтобы пользоваться инструментом PSPA. Номер счета пользователя автоматически отображается на изображении, где создан VPA, как показано на фиг. 8А. Таким образом, пользователю не нужно помнить реквизиты своего счета. Затем пользователю предлагается создать новый VPA или использовать адреса VPA, зарегистрированные им (если он ранее выполнил создание VPA). В одном варианте осуществления настоящего изобретения, если пользователь зарегистрирован в банке "xyz", то его VPA имеет код расширения "@xyz". Правила действий по определению кода расширения адресов VPA для конкретной PSPS определяются UPI (100) и/или PSPS, и он хранится на UPI-сервере и/или на PSPS-сервере. Таким образом, VPA будет иметь имя пользователя, выбранное пользователем с кодом расширения, связанным с PSPS, в которой пользователь зарегистрирован. Поэтому в случае "abc@xyz" "abc" представляет собой уникальное имя/имя пользователя, выбранное пользователем, а "xyz" представляет собой имя PSPS пользователя. Другие примеры включают Уникальное имя@HDFC, Уникальное имя@SBI, Уникальное имя@Corporation, Уникальное имя@PNB и так далее. Затем пользователь PSPS хранит данные о своем VPA и других нефинансовых данных, созданных с использованием инструмента PSPA на локальном запоминающем устройстве PSPS. В одном варианте осуществления настоящего изобретения пользователь регистрирует по меньшей мере в одном банке такие данные учетной записи, как имя учетной записи пользователя, номер учетной записи, номер Aadhaar (Aadhaar - уникальный персональный номер системы идентификации граждан и резидентов Индии), код IFSC (IFSC - код финансовой системы Индии) и тому подобное, используя инструмент PSPA, который необходим для идентификации банковского счета пользователя для совершения платежной транзакции. При успешном создании VPA пользователь может использовать VPA при передаче запросов на push-платеж или pull-платеж/данных о транзакции посредством инструмента PSPA. Кроме того, пользователь также может использовать номер учетной записи вместе с IFSC, номером Aadhaar, номером Aadhaar + номер IIN (IIN - объединенная информационная сеть) и номером мобильного телефона, а также вместе с идентификационным номером платежной системы "мобильные деньги" (MMID, или вместе только с номером своего мобильного телефона (в том случае и в тот момент, когда он подключен к системе) для оплаты посредством UPI (100).

После завершения процесса регистрации и создания VPA пользователи (плательщики и получатели платежей) имеют соответствующие VPA. Плательщик или получатель платежа использует VPA/уникальные ID, не зная названия банков или реквизитов банковского счета другого лица, для совершения платежных транзакций. Данные VPA и банковские данные всех пользователей поддерживаются соответствующими локальными запоминающими устройствами и обрабатываются соответствующими PSPS-серверами, и они не должны использоваться совместно с UPI (100).

Платежные транзакции включают инкассируемые транзакции (запрос на инкассацию) и транзакции оплаты (запрос на оплату). Инструмент PSPA предоставляет зарегистрированному пользователю различные опции на изображении дисплея его пользовательского устройства для совершения платежных транзакций, как показано на фиг. 8В. Для оплаты платежа или получения денег пользователь может выбрать любую опцию из следующих: оплата на VPA, инкассирование платежа с VPA, оплата с использованием QR-кода (QR code - код быстрого реагирования), оплата с использованием номера учетной записи в IFSC, оплата на Aadhaar, оплата на номер мобильного телефона. UPI (100) с помощью инструмента PSPA также упрощает отслеживание пользователем истории своих транзакций в UPI. Он также позволяет пользователю управлять пользовательскими VPA. Если пользователь хочет управлять своими VPA, он может выбрать опцию "управлять", отображаемую на изображении, как показано на фиг. 8В, в ответ пользователю отображается изображение, показанное на фиг. 8Е, с помощью инструмента его PSPA. Затем пользователь может выбрать: создание VPA, изменение существующего VPA или удаление существующего VPA.

Когда получатель платежа хочет инкассировать деньги у плательщика (т.е. получить деньги или совершить инкассированную транзакцию, или сделать запрос на инкассацию) (фиг. 2А), получатель платежа использует пользовательское устройство получателя платежа (102) для того, чтобы получить доступ и управление инструментом PSPA для предоставления VPA/уникального ID плательщика вместе с суммой, которую получатель хочет инкассировать у плательщика (этап 1). В одном варианте осуществления настоящего изобретения, изображение, отображаемое получателю платежа, представлено на фиг. 8D. Это изображение отображается при инициировании запроса на инкассацию (т.е. "инкассировать с VPA", как показано на фиг. 8В). При инкассации с VPA, VPA пользователя/получателя платежа загружается автоматически, поскольку пользователь уже зарегистрирован. Затем получателю платежа необходимо ввести VPA плательщика, сумму, которую необходимо инкассировать, и комментарии, если таковые имеются.

Получателю также предоставляется опция электронной инкассации платежа незамедлительно или в указанное время. Как только запрос на инкассацию отправится, он проверяется PSPS получателя платежа (106). Проверенный запрос направляется в UPI (100) вместе с зарегистрированными банковскими реквизитами получателя платежа и VPA/уникальным ID плательщика, посредством PSPS получателя платежа (106) (этап 2). UPI (100) идентифицирует PSPS плательщика (108) на основании кода расширения VPA плательщика и отправляет запрос на инкассацию в PSPS плательщика (108) (этап 3). PSPS плательщика (108) передает запрос на инкассацию плательщику посредством его инструмента PSPA с использованием пользовательского устройства плательщика (104). Плательщик принимает запрос на инкассацию и предоставляет данные аутентификации, если он согласен исполнить запрос на инкассацию, т.е. если он согласен оплатить запрашиваемую сумму получателю платежа. Плательщик проходит аутентификацию системой PSPS плательщика (108) перед совершением транзакции с использованием средства аутентификации (на фигурах не показано). Средство аутентификации включает PIN-код UPI, биометрическое сканирование, иридо-сканирование и так далее. Одно из подтверждений аутентификации предоставляется плательщиком для продолжения транзакции. Банковские реквизиты плательщика, зарегистрированные в инструменте PSPA плательщика и PSPS плательщика (108), посредством пользовательского устройства плательщика (104) передаются на UPI-сервер (100) (этап 4). Теперь в UPI (100) имеются банковские реквизиты как плательщика, так и получателя платежа на основании их адресов VPA/уникальных ID. UPI (100) использует банковские реквизиты для связи с банком-ремитентом (110) (т.е. с банком плательщика) и для дебетования желаемой суммы (этап 5 и 6), а затем для связи с банком-бенефициаром (112) (т.е. с банком получателя платежа) для кредитования этой суммы для того, чтобы завершить транзакцию (этап 7 и 8). После успешной транзакции UPI (100) отправляет информацию об успешной транзакции инструментам PSPA получателя платежа (этап 9а, 9б и 10), и плательщику, к которому получило доступ пользовательское устройство получателя платежа (102) и пользовательское устройство плательщика (104), соответственно, при этом окно с данными по транзакции всплывает на дисплеях соответствующих пользовательских устройств посредством соответствующих инструментов PSPA.

Поток транзакции в связи с запросом на инкассацию/pull-запросом включает следующие этапы (фиг. 3).

Этап 301 - получатель платежа инициирует транзакцию посредством инструмента своего PSPA на пользовательском устройстве получателя платежа (102).

Этап 302 - пользовательское устройство получателя платежа (102) инициирует запрос на инкассацию в PSPS получателя платежа (106).

Этап 303 - PSPS получателя платежа (106) проверяет данные получателя платежа и проверяет первый фактор аутентификации.

Этап 304 - PSPS получателя платежа (106) отправляет запрос на инкассацию в UPI (100).

Этап 305 - UPI (100) разрешает адрес плательщика двумя способами:

а) если адрес имеет глобальные идентификаторы (например, номер Мобильного телефона, уникальный ID, номер учетной записи и так далее), то PSPS запрашивает UPI (100) об ожидающих сообщениях посредством интерфейса прикладного программирования (API) по данному номеру мобильного телефона или по номеру Aadhaar, или по номеру учетной записи и IFSC;

б) если адрес имеет виртуальный адрес, предложенный PSPS плательщика (108), то UPI (100) отправляет запрос в PSPS плательщика (108) на перевод адреса.

Этап 306 - в случае этапа 305b, PSPS плательщика (108) отправляет уведомление плательщику, который принимает или отклоняет запрос на основании правил действий, установленных на его стороне.

Этап 307 - в случае этапа 305b, при приеме запроса на инкассацию, PSPS плательщика (108) инициирует запрос пользовательскому устройству плательщика (104) на ввод подтверждений аутентификации плательщика. Плательщик предоставляет подтверждения аутентификации на пользовательском устройстве плательщика (104).

Этап 308 - в случае этапа 305b, PSPS плательщика (108) загружает данные плательщика и отвечает UPI (100).

Этап 309 - UPI (100) отправляет дебетовый запрос на дебетование счета поставщика (110).

Этап 310 - поставщик счета аутентифицирует плательщика на основании предоставленных подтверждений.

Этап 311 - поставщик счета дебетует счет плательщика.

Этап 312 - поставщик счета отправляет дебетовый ответ в UPI (100).

Этап 313 - UPI (100) отправляет кредитовый запрос поставщику кредитового счета (112).

Этап 314 - поставщик счета кредитует счет на основании данных получателя платежа.

Этап 315 - поставщик счета отправляет кредитовый ответ в UPI (100).

Этап 316 - UPI (100) отправляет подтверждающий ответ в PSPS плательщика (108).

Этап 317 - UPI (100) отправляет ответ на платеж в PSPS получателя платежа (106).

Этап 318 - PSPS получателя платежа (106) уведомляет получателя платежа.

Когда плательщик хочет отправить деньги получателю платежа (т.е. оплатить деньги или оплатить транзакцию, или сделать Push-запрос) (фиг. 2B), плательщик использует пользовательское устройство

плательщика (104) для того, чтобы получить доступ и управление инструментом PSPA для предоставления авторизованного VPA получателя платежа вместе с суммой, которую плательщик хочет отправить получателю платежа (этап 1). В одном варианте осуществления настоящего изобретения, изображение, отображаемое получателю платежа, представлено на фиг. 8С. Это изображение отображается при иницировании push-запроса/запроса на оплату (т.е. "Оплатить на VPA", как показано на фиг. 8В). При оплате на VPA VPA пользователя/плательщика загружается автоматически, поскольку пользователь уже зарегистрирован в инструменте PSPA с данными о своей PSPS. Затем плательщику необходимо ввести VPA получателя платежа, сумму, которую необходимо инкассировать, и комментарии, если таковые имеются. После отправки запроса на оплату плательщик может быть аутентифицирован PSPS плательщика (108) перед совершением транзакции с использованием средства аутентификации. Средство аутентификации включает PIN-код UPI, биометрическое сканирование, иридо-сканирование и так далее. Одно из подтверждений аутентификации предоставляется плательщиком. Аутентификация плательщика направляется в UPI (100) вместе с зарегистрированными банковскими реквизитами плательщика и VPA получателя платежа посредством PSPS плательщика (108) (этап 2). UPI (100) идентифицирует PSPS получателя платежа (106) на основании кода расширения VPA получателя платежа и отправляет запрос в PSPS получателя платежа (106) (этап 3). PSPS получателя платежа (106) авторизует банковские реквизиты, зарегистрированные в инструменте PSPA получателя платежа, в PSPS получателя платежа (106) посредством пользовательского устройства получателя платежа (102), и возвращает банковские реквизиты на UPI-сервер (100) (этап 4). Теперь в UPI (100) имеются банковские реквизиты как плательщика, так и получателя платежа на основании их адресов VPA/уникальных ID. UPI (100) использует банковские реквизиты для связи с банком-ремитентом (110) (т.е. с банком плательщика) и дебетования желаемой суммы (этап 5 и 6), а затем для связи с банком-бенефициаром (112) (т.е., с банком получателя платежа) для кредитования этой суммы для того, чтобы завершить транзакцию (этап 7 и 8). После успешной транзакции, UPI (100) отправляет информацию об успешной транзакции инструментам PSPA плательщика (этап 9а, 9б и 10), и получателю платежа, к которому получило доступ пользовательское устройство плательщика (104) и пользовательское устройство получателя платежа (102), соответственно, при этом окно с данными по транзакции всплывает на дисплеях соответствующих пользовательских устройств посредством соответствующих инструментов PSPA.

UPI (100), в конце дня, когда все финансовые и нефинансовые транзакции завершены, выполняет расчет всех платежных транзакций, которые были совершены между всеми системами PSPS, зарегистрированными в EPS (1000). В одном варианте осуществления настоящего изобретения, плательщик использует инструмент PSPA, который отличается от инструмента PSPA получателя платежа. В другом варианте осуществления настоящего изобретения плательщик использует тот же инструмент PSPA, что и получатель платежа.

Поток транзакции в связи с запросом на оплату/push-запросом включает следующие этапы (фиг. 4).

Этап 401 - плательщик иницирует транзакцию посредством инструмента своего PSPA на пользовательском устройстве плательщика (104).

Этап 402 - плательщик предоставляет подтверждения аутентификации на пользовательском устройстве плательщика (104).

Этап 403 - пользовательское устройство плательщика (104) иницирует запрос на оплату в PSPS плательщика (108).

Этап 404 - PSPS плательщика (108) проверяет данные плательщика и проверяет первый фактор аутентификации.

Этап 405 - PSPS плательщика (108) отправляет запрос на оплату в UPI (100).

Этап 406 - UPI (100) разрешает адрес плательщика следующими двумя способами:

а) если адрес имеет глобальные идентификаторы (например, номер мобильного телефона, уникальный ID, номер учетной записи и так далее), то адрес получателя платежа может быть разрешен посредством центрального картографа UPI (100);

б) если адрес имеет виртуальный адрес, предложенный PSPS получателя платежа (106), то UPI (100) отправляет запрос в PSPS получателя платежа (106) на перевод адреса.

Этап 407 - в случае 406b, PSPS получателя платежа (106) принимает или отклоняет запрос на основании правил действий, установленных на его стороне.

Этап 408 - в случае 406b, при принятии запроса на оплату PSPS получателя платежа (106) загружает данные плательщика и отвечает UPI (100).

Этап 409 - UPI (100) отправляет дебетовый запрос на дебетование счета поставщика (114).

Этап 410 - поставщик счета аутентифицирует плательщика на основании предоставленных подтверждений.

Этап 411 - поставщик счета дебетует счет плательщика.

Этап 412 - поставщик счета отправляет дебетовый ответ в UPI (100).

Этап 413 - UPI (100) отправляет кредитовый запрос поставщику кредитового счета (112).

Этап 414 - поставщик счета кредитует счет на основании данных получателя платежа.

Этап 415 - поставщик счета отправляет кредитовый ответ в UPI (100).

Этап 416 - UPI (100) отправляет подтверждающий ответ в PSPS получателя платежа (106).

Этап 417 - UPI (100) отправляет ответ на платеж в PSPS плательщика (108).

Этап 418 - PSPS плательщика (108) уведомляет плательщика.

EPS (1000) использует различные способы аутентификации. В одном варианте осуществления изобретения EPS (1000) использует способ двухфакторной аутентификации с одним кликом, как показано в табл.1 ниже.

Таблица 1

Аутентификация	Регистрация	Авторизовано	Транзакция	Авторизовано
1-й фактор	Мобильное устройство / Номер (исходящее зашифрованное SMS-сообщение)	PSPS	Отпечаток устройства	PSPS
2-й фактор	ОТР	Эмитент	PIN-код UPI или биометрические характеристики	Эмитент

В одном варианте осуществления настоящего изобретения каждая PSPS (1004) содержит модуль аутентификации (на фигурах не показано), выполненный с возможностью предоставления двухфакторной аутентификации. Модуль аутентификации содержит первый фактор аутентификации и второй фактор аутентификации. Первый фактор аутентификации принимает предварительно зарегистрированный уникальный номер, формирует пользователя, зарегистрированного в с PSPS (1004), для проверки и связи зарегистрированного пользователя с зарегистрированным пользовательским устройством (1006), путем сопоставления принятого от зарегистрированного пользователя предварительно зарегистрированного уникального номера с информационными данными о пользователе, хранящимися на локальном запоминающем устройстве (1004a), тем самым обеспечивая первый фактор аутентификации. Второй фактор аутентификации выполнен с возможностью приема PIN-кода UPI и/или биометрических характеристик, введенных зарегистрированным пользователем, для аутентификации зарегистрированного пользователя, путем сопоставления принятого PIN-кода UPI и/или введенных биометрических характеристик с информационными данными о пользователе, тем самым обеспечивая второй фактор аутентификации.

Как видно из табл. 1, в первом факторе аутентификации, во время регистрации в инструменте PSPA, зашифрованное SMS-сообщение инициируется пользовательским устройством/мобильным телефоном пользователя и передается в PSPS, в которой зарегистрирован пользователь. PSPS проверяет уникальный номер (номер мобильного телефона или международный идентификатор аппаратуры мобильной связи (IMEI) и так далее) пользовательского устройства (этот уникальный номер предварительно сохраняется в качестве информационных данных о пользователе с помощью PSPS во время регистрации пользователя) и связывает уникальный номер с учетной записью пользователя. Если покупатель зарегистрирован в мобильном банкинге, то он будет использовать свой PIN-код UPI или биометрические характеристики во втором факторе аутентификации. Если покупатель хочет зарегистрироваться в мобильном банкинге, то он может установить PIN-код UPI, используя последние 6 цифр дебетовой карты и даты истечения срока дебетовой карты вместе с ОТР, созданным эмитентом, или любой другие аналогичные соответствующие проверочные данные. В последующей транзакции отпечаток устройства может использоваться для авторизации системой PSPS. Во время второго фактора аутентификации PIN-код UPI или биометрические характеристики запрашиваются у пользователя, который авторизован эмитентом в последующей транзакции, для аутентификации пользователя.

Фиг. 5 сопроводительного чертежа показывает диаграмму потока, показывающую платежную транзакцию, совершаемую между водителем такси и его пассажиром. В примерном варианте осуществления система по настоящему изобретению используется водителем такси для инкассации платы за услуги, предоставленные им своему пассажиру/покупателю. Когда такси достигает желаемого места назначения, водитель такси (в данном случае получатель платежа) может использовать свое пользовательское устройство (502), чтобы получить/инкассировать платеж (плату за услуги такси) от пассажира с использова-

нием системы по настоящему изобретению. Пассажир предоставляет свой VPA, который вводится водителем такси в инструмент PSPA получателя платежа вместе с запросом на инкассирование на пользовательском устройстве водителя такси (502). VPA вместе с данными счета водителя такси предоставляется UPI (500) системой PSPS (506) водителя такси (получателя платежа) (этап 51). UPI (500) идентифицирует PSPS/банк пассажира (плательщика) посредством VPA и направляет запрос на инкассацию в PSPS пассажира (508) (этап 52). PSPS пассажира (508) отправляет уведомление о запросе на инкассацию инструменту PSPA пассажира на пользовательском устройстве пассажира (504) (этап 53) на основании того, какие подтверждения аутентификации предоставляются пассажиром для принятия запроса на инкассацию (этап 54). В одном варианте осуществления настоящего изобретения, аутентификация предоставляется путем ввода PIN-кода UPI с использованием инструмента PSPA на пользовательском устройстве пассажира (504). По получении подтверждения от пассажира (получателя платежа), PSPS пассажира (508) проверяет данные о пассажире и отправляет финансовые данные UPI (500) для дебетования банковского счета пассажира (плательщика) (этап 55). Затем дебетовый запрос отправляется PSPS/банку пассажира (ремитенту) (510), и запрашиваемая сумма списывается по дебету с банковского счета пассажира (ремитента) (510) (этап 56 и 57) посредством UPI (500). Затем UPI (500) отправляет кредитовый запрос PSPS водителя такси/банку (бенефициару) (512) на кредитование нужной суммы (этап 58) и получает сообщение об успешном кредитовании от PSPS водителя такси/банка (бенефициара) (512) об успешном кредитовании (этап 59). Затем подтверждение об успешной транзакции передается посредством UPI (500) пассажиру (плательщику) (этап 50a) и водителю такси (получателю платежа) (50b) посредством инструментов своих соответствующих PSPA.

EPS (1000) по настоящему изобретению может использоваться доставщиком (доставка еды, доставка одежды и так далее) для того, чтобы избежать проблем, связанных с оплатой наличными при доставке (COD). Она обеспечивает двухфакторную аутентификацию с одним кликом, при этом транзакция может быть авторизована путем ввода только PIN-кода UPI.

На фиг. 6 показана диаграмма потока, показывающая платежную транзакцию по переводу денег, совершаемую с помощью EPS (1000), которая используется отправителем (плательщиком) для совершения push-платежа. Отправитель использует свое пользовательское устройство (604) для ввода запроса на оплату, включая VPA получателя (получателя платежа) и PIN-код UPI банка-эмитента вместе с суммой, которая должна быть отправлена в банк получателя (этап 61). Затем реквизиты счета отправителя, PIN-код UPI и VPA получателя предоставляются UPI (600) посредством PSPS отправителя (608), с использованием инструмента своего PSPA (этап 62). UPI (600) идентифицирует дестриптор/данные PSPS получателя (получателя платежа/бенефициара) и отправляет запрос на оплату в PSPS получателя (606) (этап 63). PSPS получателя (606) отвечает на финансовый адрес бенефициара (т.е. финансовый адрес получателя платежа) (этап 64). На основании ответа UPI (600) отправляет реквизиты счета отправителя (плательщика) и PIN-код вместе с дебетовым запросом в PSPS/банк отправителя (610) (этап 65) и получает успешный дебетовый ответ (этап 66). При получении дебетового ответа, UPI (600) отправляет кредитовый запрос в PSPS/банк получателя/получателя платежа (612) (этап 67) и получает успешный кредитовый ответ (этап 68). Затем подтверждение об успешной транзакции отправляется в PSPS получателя/получателя платежа (этап 69) и отправителю, посредством PSPS (608) отправителя и его пользовательского устройства (604) (этап 60).

Плательщик/отправитель/продавец и получатель платежа/получатель/покупатель могут иметь одинаковые PSPS. На фиг. 7 показана диаграмма потока, показывающая трехстороннюю коммерческую транзакцию между покупателем и продавцом, у которых имеется одинаковая PSPS. Покупатель (710) зарегистрирован в UPI (700) системы по настоящему изобретению с использованием инструмента PSPA на своем пользовательском устройстве (702). Поскольку PSPS (704) покупателя и продавца одинаковые, то виртуальные адреса как продавца, так и покупателя доступны в PSPS (704). Когда запрос (push-запрос или pull-запрос) выполняется с использованием инструмента PSPA, то запрос отправляется в PSPS (704), который (в данном случае) является общим как для продавца, так и для покупателя (этап 71). В одном варианте осуществления настоящего изобретения запрос содержит справочный ID (VPA пользователя), сумму и ID продавца. Поскольку виртуальные адреса доступны в PSPS (704), то финансовые адреса, лежащие в основе виртуальных адресов, предоставляются в UPI (700) посредством PSPS (704) (этап 72). Затем UPI (700) отправляет дебетовый запрос эмитенту/PSPS плательщика/банку (706) (этап 73) и принимает дебетовый ответ (этап 74) на основании push-запроса или pull-запроса. Затем UPI (700) отправляет кредитовый запрос эквайеру/PSPS получателя платежа/банку (708) (этап 75) и получает ответ об успешном кредите от эквайера/PSPS/банка получателя платежа (708) (этап 76). UPI (700) передает успешную транзакцию пользователю посредством его пользовательского устройства (702) с использованием PSPS (704) (этап 77 и 78).

Настоящее изобретение предусматривает способ совершения электронных платежей, который упрощает совершение платежных транзакций между множеством пользователей. Этот способ содержит следующие этапы:

хранение в оперативном запоминающем устройстве набора предварительно заданных правил действий;

обработка операционным процессором предварительно заданных правил действий для получения набора команд управления работой системы;

регистрация пользователей во множестве систем операторов платежного сервиса (PSPS), выполненных с возможностью регистрации в системе электронных платежей (EPS) (1000), причем каждая PSPS содержит следующие этапы:

хранение на локальном запоминающем устройстве информационных данных о пользователе, относящихся к пользователям, зарегистрированным в PSPS,

упрощение с помощью по меньшей мере одной поисковой таблицы, сопоставления данных, введенных покупателем, информационных данных о пользователе и о зарегистрированном пользователе, и предоставление PSPS-сервера;

связывание каждого пользовательского устройства из множества пользовательских устройств с одним из зарегистрированных пользователей и регистрация в качестве части информационных данных о пользователе;

связывание и размещение на своем ресурсе каждого инструмента приложения оператора платежного сервиса (PSPA) из множества инструментов PSPA, с помощью PSPS-сервера системы PSPS, зарегистрированной в EPS, и содержание элементов, которые загружаются и хранятся в пользовательском устройстве зарегистрированного пользователя, независимо от того, зарегистрирован ли зарегистрированный пользователь в PSPS, связанной с инструментом PSPA, или нет, и в дальнейшем упрощение, посредством каждого инструмента PSPA, генерации и приема сигналов по данным о транзакции, относящихся к запросам на платеж от зарегистрированных пользователей, а также к кредитовым и/или дебетовым счетам зарегистрированных пользователей на основании запросов, причем загружаемые элементы каждого инструмента PSPA содержат этапы:

разрешение посредством модуля регистрации регистрации пользовательского устройства в зарегистрированной PSPS, связанной с инструментом PSPA во взаимно-однозначном соответствии, и

предоставление возможности посредством модуля создания виртуального платежного адреса (VPA) зарегистрированному пользователю создать уникальный VPA, который включает идентификацию PSPS, в которой зарегистрирован зарегистрированный пользователь, и в дальнейшем предоставление возможности пользовательскому устройству передать уникальный VPA на локальное запоминающее устройство PSPS, в которой пользователь зарегистрирован, в качестве части информационных данных о пользователе от зарегистрированного пользователя; и

упрощение посредством Унифицированного платежного интерфейса (UPI) регистрации PSPS в EPS и управляемого перемещения сигналов по данным о транзакции, выборочно, между системами PSPS для осуществления платежа от одного зарегистрированного пользователя к другому зарегистрированному пользователю в одинаковых или разных системах PSPS, причем UPI содержит этапы:

предоставление модуля расчетов, выполненного с возможностью взаимодействия со множеством систем PSPS для периодического сопоставления кредитовых и дебетовых транзакций и генерирования инструкций по чистому кредиту и дебету между зарегистрированными системами PSPS.

UPI дополнительно содержит следующие этапы:

прием получателем сигналов по данным о транзакции, относящихся к запросам на платеж от зарегистрированных пользовательских устройств посредством любого из инструментов PSPA, причем каждый запрос содержит VPA первого зарегистрированного пользователя, VPA второго зарегистрированного пользователя и сумму транзакции;

анализирование анализатором сигналов по данным о транзакции для получения проанализированных сигналов,

извлечение и идентификацию из проанализированных сигналов, с помощью извлекателя идентификатора, информации, относящейся к PSPS первого зарегистрированного пользователя и PSPS второго зарегистрированного пользователя,

передача передатчиком сигналов по данным о транзакции идентифицированными соответствующими системами PSPS для упрощения списания кредитового платежа со счета первого зарегистрированного пользователя на счет второго зарегистрированного пользователя или зачисления дебетового платежа на счет первого зарегистрированного пользователя со счета второго зарегистрированного пользователя, выборочно, на основании содержимого данных проанализированных сигналов.

Каждая PSPS дополнительно содержит этап предоставления двухфакторной аутентификации модулем аутентификации. Этап предоставления двухфакторной аутентификации содержит следующие этапы:

прием посредством первого фактора аутентификации предварительно зарегистрированного уникального номера от пользователя, зарегистрированного в PSPS, для проверки и связи зарегистрированного пользователя с зарегистрированным пользовательским устройством путем сопоставления принятого от зарегистрированного пользователя предварительно зарегистрированного уникального номера с информационными данными о пользователе, хранящимися на локальном запоминающем устройстве, тем самым обеспечивая первый фактор аутентификации, и

прием посредством второго фактора аутентификации PIN-кода UPI и/или биометрических характеристик, введенных зарегистрированным пользователем, для аутентификации зарегистрированного поль-

зователя путем сопоставления принятого PIN-кода UPI и/или введенных биометрических характеристик с информационными данными о пользователе, тем самым обеспечивая второй фактор аутентификации.

Даже если покупатель и продавец используют одинаковую PSPS, они оба могут иметь множество различных инструментов PSPA на своих пользовательских устройствах. Для примера, набор инструментальных средств разработки программ (SDK) PSPA встроен в инструмент PSPA продавца, и различные инструменты PSPA доступны покупателю. В том случае, когда продавец имеет намерение/создает запрос, на пользовательском устройстве клиента отображаются все инструменты UPI PSPA с тем, чтобы покупатель мог выбрать одинаковый с продавцом инструмент PSPA. Как показано на фиг. 7, в этом примере также виртуальные адреса как продавца, так и покупателя доступны в PSPS, и транзакция происходит таким же образом, как описано выше.

EPS (1000), предусмотренная в настоящем изобретении, может использоваться реальными магазинами/продавцами для совершения транзакций, включая оплату поставщикам овощной продукции, оплату за продукты в магазине, оплату за проезд в такси/автомобиле/автобусе/поезде/оплату за авиаперелет, оплату в ресторанах/магазинах/за заправку бензина, оплату за учебу различным учебным заведениям, оплату за проезд в пунктах сбора пошлины во время путешествия, оплату поставщикам молочной продукции/разносчикам газет, пожертвования доверительному фонду/храму/фонду взаимопомощи/НПО, оплату в торговом центре и тому подобное. EPS (1000) также может использоваться для совершения оплаты коммунальных услуг, включая оплату различных счетов, таких как счета за электричество, воду, телефон, кредитную карту и так далее, для выставления и оплаты счетов за ремонт квартиры, для выставления и оплаты счетов за учебу в школе, для уплаты страховой премии, погашения кредита в расщелку, погашения автокредита посредством внешнего интерфейса компьютера (EMI) и тому подобное.

Кроме того, онлайн-продавцы также могут использовать EPS (1000) для совершения транзакций в электронной коммерции, включая COD-платежи, для платежей во встроенном приложении (In-App), в онлайн-трейдинге, за мобильное пополнение счета по газетному объявлению с использованием приложения "Scan N Pay", в электронной коммерции (инкассация/оплата) - платеж посредством UPI после оформления заказа, для платежей за бронирование билетов в кино и тому подобное. Кроме того, она также может использоваться для совершения транзакций при непосредственном соединении двух устройств для перевода денег (и оплата, и получение денег), для платежей физическому лицу/друзьям, для разделения счетов с друзьями, для выплаты заработной платы водителю, для платежей на номер Aadhaar/номер мобильного телефона на основании внутреннего перевода на другой банковский счет.

Технический прогресс.

Настоящее изобретение, описанное выше, имеет ряд технических преимуществ, включая, но этим не ограничиваясь, реализацию системы электронных платежей, которая

упрощает отправку и получение денег более простым способом с использованием пользовательских устройств;

предоставляет унифицированный платежный интерфейс (UPI);

предоставляет возможность пользователю получать/инкассировать платежи со счетов заинтересованных физических/юридических лиц;

проста в использовании как для плательщиков, так и для получателей платежей;

предоставляет возможность совершения платежных транзакций между плательщиком и получателем платежа без необходимости обязательного предоставления банковской информации и реквизитов банковского счета друг друга;

предоставляет возможность пользователю отправлять и получать деньги с помощью виртуального платежного адреса;

предоставляет безопасное совершение платежей на основании единственного/уникального идентификатора;

устраняет риск хранения виртуального адреса покупателя, как на карточках;

может использоваться покупателями, которые не имеют кредитной/дебетовой карты;

подходит для электронной коммерции и мобильной коммерции;

решает проблему инкассации COD;

предоставляет возможность совершения платежей за покупки во встроенном приложении (IAP);

обеспечивает конфиденциальность путем совместного использования только виртуального адреса и никакой другой конфиденциальной информации;

упрощает установление множества утилит - при оплате наличными при доставке/при разделении/совместном использовании счетов/при оплате/переводe денег продавцу;

авторизует транзакцию путем введения только PIN-кода UPI или биометрических характеристик, или ID пользователя (UID), или путем проведения иридо-сканирования и так далее;

работает посредством различных интерфейсов, где запрос на платеж может быть сгенерирован на интернет-интерфейсе и авторизован на мобильном интерфейсе (App).

Варианты осуществления настоящего изобретения и различные признаки и подробное описание их преимуществ поясняются со ссылкой на неограничивающие варианты осуществления настоящего изобретения, представленные в нижеследующем описании. Подробное описание хорошо известных компо-

ентов и способов обработки опущены в настоящем документе, чтобы чрезмерно не затруднять понимание вариантов осуществления настоящего изобретения. Используемые в настоящем документе примеры предназначены лишь для упрощения понимания способов осуществления вариантов по настоящему изобретению и в дальнейшем для предоставления возможности специалистами в данной области техники использования на практике вариантов осуществления изобретения по настоящему документу. Соответственно, эти примеры не следует истолковывать как ограничивающие объем вариантов осуществления изобретения по настоящему документу.

Вышеприведенное описание конкретных вариантов осуществления настоящего изобретения настолько полно раскрывает общий характер вариантов осуществления изобретения по документу, что другие могут, применяя знания существующего уровня техники, легко модифицировать и/или адаптировать для различных применений такие конкретные варианты осуществления настоящего изобретения, не отходя от общей концепции, и, следовательно, такие адаптации и модификации следует истолковывать по смыслу и в серии эквивалентов раскрытых вариантов осуществления настоящего изобретения. Следует понимать, что используемая в настоящем документе фразология или терминология предназначена для описания, а не для ограничения. Таким образом, хотя варианты осуществления изобретения описаны в настоящем документе с точки зрения предпочтительных вариантов осуществления настоящего изобретения, специалисты в данной области техники поймут, что варианты осуществления изобретения по настоящему документу могут быть осуществлены на практике с модификацией в пределах существа и объема вариантов осуществления изобретения, как они описаны в настоящем документе.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система электронных платежей (EPS) (1000) для упрощения совершения платежных транзакций между множеством пользователей, включающая

оперативное запоминающее устройство (1002a), выполненное с возможностью хранения набора предварительно заданных правил действий;

операционный процессор (1002b), выполненный с возможностью взаимодействия с вышеупомянутым оперативным запоминающим устройством (1002a) для приема и обработки вышеупомянутых предварительно заданных правил действий для получения набора команд управления работой системы;

множество Систем операторов платежного сервиса (PSPS), выполненных с возможностью регистрации пользователей и выполненных с дополнительной возможностью регистрации в вышеупомянутой EPS (1000), причем каждая PSPS (1004) содержит

локальное запоминающее устройство (1004a), выполненное с возможностью хранения информационных данных о пользователе, относящихся к пользователям, зарегистрированным в вышеупомянутой PSPS (1004);

по меньшей мере одну поисковую таблицу (1004b), выполненную с возможностью упрощения сопоставления данных, введенных покупателем, информационных данных о пользователе и о зарегистрированным пользователе; и

PSPS-сервер (1004c);

множество пользовательских устройств, причем каждое пользовательское устройство (1006) связано с одним из вышеупомянутых зарегистрированных пользователей и зарегистрировано в качестве части информационных данных о пользователе;

инструменты Приложения оператора платежного сервиса (PSPA), причем каждый инструмент PSPA (1008) связан и размещен на своем ресурсе PSPS-сервером (1004c) системы PSPS (1004), зарегистрированной в EPS (1000), и содержит элементы, которые загружаются и хранятся в пользовательском устройстве (1006) зарегистрированного пользователя независимо от того, зарегистрирован ли зарегистрированный пользователь в PSPS, связанной с вышеупомянутым инструментом PSPA (1008), или нет, причем каждый инструмент PSPA (1008) выполнен с возможностью упрощения генерации и приема сигналов по данным о транзакции, относящихся к запросам на платежи от вышеупомянутых зарегистрированных пользователей, а также к кредитовым и/или дебетовым счетам вышеупомянутых зарегистрированных пользователей на основании вышеупомянутых запросов, причем вышеупомянутые загружаемые элементы каждого инструмента PSPA (1008) содержат

модуль регистрации (1008a), выполненный с возможностью разрешения регистрации пользовательского устройства (1006) в зарегистрированной PSPS (1004), связанной с инструментом PSPA (1008) во взаимно-однозначном соответствии; и

модуль создания виртуального платежного адреса (VPA) (1008b), выполненный с возможностью создания зарегистрированному пользователю уникального VPA, который содержит идентификацию PSPS, в которой зарегистрирован зарегистрированный пользователь, и в дальнейшем предоставить возможность пользовательскому устройству (1006) передавать вышеупомянутый уникальный VPA на локальное запоминающее устройство (1004a) системы PSPS (1004), в которой зарегистрирован пользователь, как части информационных данных о пользователе от зарегистрированного пользователя; и

унифицированный платежный интерфейс UPI (100), выполненный с возможностью упрощения ре-

гистрации PSPS (1004) в вышеупомянутой EPS (1000) и выполненный с дополнительной возможностью упрощения управляемого перемещения сигналов по данным о транзакции, выборочно, между системами PSPS для осуществления платежа от одного зарегистрированного пользователя к другому зарегистрированному пользователю в одинаковых или разных системах PSPS, причем вышеупомянутый UPI (100) содержит модуль расчетов (100a), выполненный с возможностью взаимодействия с вышеупомянутым множеством систем PSPS для периодического сопоставления кредитовых и дебетовых транзакций и генерирования инструкций по чистому кредиту и дебету между зарегистрированными системами PSPS.

2. EPS (1000) по п.1, в которой вышеупомянутый UPI (100) дополнительно содержит

приемник (100b), выполненный с возможностью приема сигналов по данным о транзакции, относящихся к запросам на платежи от зарегистрированных пользовательских устройств посредством любого из инструментов PSPA, причем каждый запрос содержит VPA первого зарегистрированного пользователя, VPA второго зарегистрированного пользователя и сумму транзакции;

анализатор (100c), выполненный с возможностью анализа вышеупомянутых сигналов по данным о транзакции для получения проанализированных сигналов;

извлекатель идентификатора (100d), выполненный с возможностью извлечения и идентификации из проанализированных сигналов информации, относящейся к PSPS первого зарегистрированного пользователя и к PSPS второго зарегистрированного пользователя; и

передатчик (100e), выполненный с возможностью передачи вышеупомянутых сигналов по данным о транзакции, идентифицированных соответствующими системам PSPS, для упрощения списания кредитового платежа со счета первого зарегистрированного пользователя на счет второго зарегистрированного пользователя или зачисления дебетового платежа на счет первого зарегистрированного пользователя со счета второго зарегистрированного пользователя, выборочно, на основании содержимого данных проанализированных сигналов.

3. EPS (1000) по п.1, в которой каждая PSPS (1004) дополнительно содержит модуль аутентификации, выполненный с возможностью предоставления двухфакторной аутентификации и содержащий

первый фактор аутентификации, выполненный с возможностью приема предварительно зарегистрированного уникального номера, формирования зарегистрированного пользователя в вышеупомянутой PSPS (1004) для проверки и связи зарегистрированного пользователя с зарегистрированным пользовательским устройством (1006), путем сопоставления принятого от зарегистрированного пользователя предварительно зарегистрированного уникального номера с информационными данными о пользователе, хранящимися на вышеупомянутом локальном запоминающем устройстве (1004a), тем самым обеспечивая первый фактор аутентификации; и

второй фактор аутентификации, выполненный с возможностью приема PIN-кода UPI и/или биометрических характеристик, введенных зарегистрированным пользователем, для аутентификации зарегистрированного пользователя путем сопоставления принятого PIN-кода UPI и/или введенных биометрических характеристик с вышеупомянутыми информационными данными о пользователе, тем самым обеспечивая второй фактор аутентификации.

4. EPS (1000) по п.2, в которой вышеупомянутый UPI (100) дополнительно содержит сервер транзакций для обработки сигналов по данным о транзакции, сервер авторизации для авторизации пользователя и UPI-сервер для обработки сохраненного набора правил действий для идентификации зарегистрированных систем PSPS.

5. Способ совершения электронных платежей для упрощения совершения платежных транзакций между множеством пользователей, включающий следующие этапы:

хранение в оперативном запоминающем устройстве набора предварительно заданных правил действий;

обработка операционным процессором вышеупомянутых предварительно заданных правил действий для получения набора команд управления работой системы;

регистрация пользователей во множестве Систем операторов платежного сервиса (PSPS) для регистрации в Системе электронных платежей (EPS) (1000), причем каждая PSPS содержит следующие этапы:

хранение на локальном запоминающем устройстве информационных данных о пользователе, относящихся к пользователям, зарегистрированным в вышеупомянутой PSPS;

упрощение с помощью по меньшей мере одной поисковой таблицы сопоставления данных, введенных покупателем, информационных данных о пользователе и о зарегистрированном пользователе; и

предоставление PSPS-сервера;

связывание каждого пользовательского устройства из множества пользовательских устройств с одним из вышеупомянутых зарегистрированных пользователей и регистрация в качестве части информационных данных о пользователе;

связывание и размещение на своем ресурсе каждого инструмента Приложения оператора платежного сервиса (PSPA) из множества инструментов PSPA с помощью PSPS-сервера системы PSPS, зарегистрированной в вышеупомянутой EPS, и содержание элементов, которые загружают и хранят в пользовательском устройстве зарегистрированного пользователя, независимо от того, зарегистрирован ли зарегистрированный пользователь в PSPS, связанной с вышеупомянутым инструментом PSPA, или нет, и уп-

рошение в дальнейшем, посредством каждого инструмента PSPA, генерации и приема сигналов по данным о транзакции, относящихся к запросам на платежи от вышеупомянутых зарегистрированных пользователей, а также к кредитовым и/или дебетовым счетам вышеупомянутых зарегистрированных пользователей на основании вышеупомянутых запросов, причем вышеупомянутые загружаемые элементы каждого инструмента PSPA содержат следующие этапы:

разрешение, посредством модуля регистрации регистрации пользовательского устройства в зарегистрированной PSPS, связанной с инструментом PSPA во взаимно-однозначном соответствии; и

предоставление возможности посредством модуля создания виртуального платежного адреса (VPA) зарегистрированному пользователю создавать уникальный VPA, который содержит идентификацию PSPS, в которой зарегистрирован зарегистрированный пользователь, и в дальнейшем предоставление возможности пользовательскому устройству передавать вышеупомянутый уникальный VPA на локальное запоминающее устройство системы PSPS, в которой пользователь зарегистрирован, в качестве части информационных данных о пользователе от зарегистрированного пользователя; и

упрощение посредством Унифицированного платежного интерфейса (UPI) регистрации PSPS в вышеупомянутой EPS и управляемого перемещения сигналов по данным о транзакции, выборочно, между системами PSPS для осуществления платежа от одного зарегистрированного пользователя к другому зарегистрированному пользователю в одинаковых или разных системах PSPS, причем UPI содержит следующий этап:

предоставление модуля расчетов для взаимодействия с вышеупомянутым множеством систем PSPS для периодического сопоставления кредитовых и дебетовых транзакций и генерирования инструкций по чистому кредиту и дебету между зарегистрированными системами PSPS.

6. Способ по п.5, в котором вышеупомянутый UPI дополнительно содержит

прием получателем сигналов по данным о транзакции, относящихся к запросам на платежи от зарегистрированных пользовательских устройств посредством любого из инструментов PSPA, причем каждый запрос содержит VPA первого зарегистрированного пользователя, VPA второго зарегистрированного пользователя и сумму транзакции;

анализирование анализатором вышеупомянутых сигналов по данным о транзакции для получения проанализированных сигналов;

извлечение и идентификация из проанализированных сигналов с помощью извлекателя идентификатора информации, относящейся к PSPS первого зарегистрированного пользователя и PSPS второго зарегистрированного пользователя;

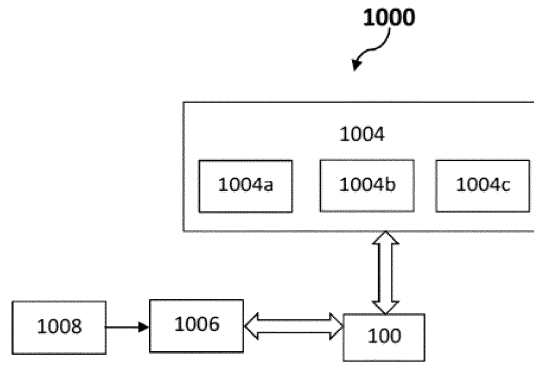
передача передатчиком вышеупомянутых сигналов по данным о транзакции идентифицированным соответствующим системам PSPS для упрощения списания кредитового платежа со счета первого зарегистрированного пользователя на счет второго зарегистрированного пользователя или зачисления дебетового платежа на счет первого зарегистрированного пользователя со счета второго зарегистрированного пользователя, выборочно, на основании содержимого данных проанализированных сигналов.

7. Способ по п.5, в котором каждая PSPS дополнительно содержит

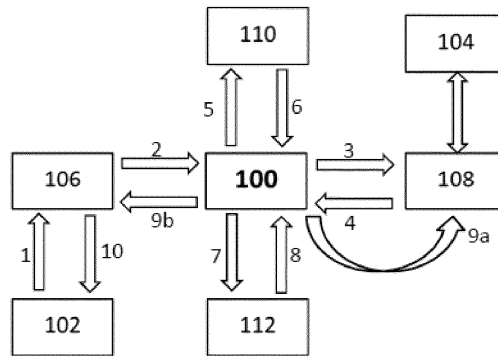
предоставление двухфакторной аутентификации модулем аутентификации, причем вышеупомянутый этап предоставления двухфакторной аутентификации содержит следующие этапы:

прием посредством первого фактора аутентификации предварительно зарегистрированного уникального номера от пользователя, зарегистрированного в вышеупомянутой PSPS, для проверки и связи зарегистрированного пользователя с зарегистрированным пользовательским устройством, путем сопоставления принятого от зарегистрированного пользователя предварительно зарегистрированного уникального номера с информационными данными о пользователе, хранящимися на вышеупомянутом локальном запоминающем устройстве, тем самым обеспечивая первый фактор аутентификации; и

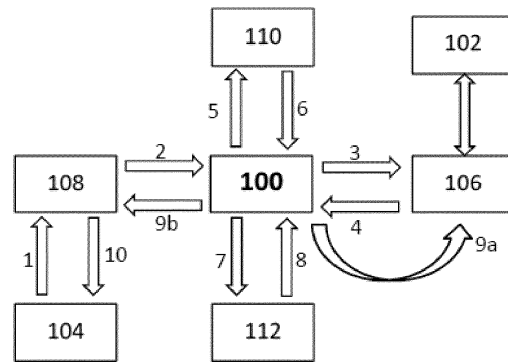
прием посредством второго фактора аутентификации PIN-кода и/или биометрических характеристик, введенных зарегистрированным пользователем, для аутентификации зарегистрированного пользователя путем сопоставления принятого PIN-кода и/или введенных биометрических характеристик с вышеупомянутыми информационными данными о пользователе, тем самым обеспечивая второй фактор аутентификации.



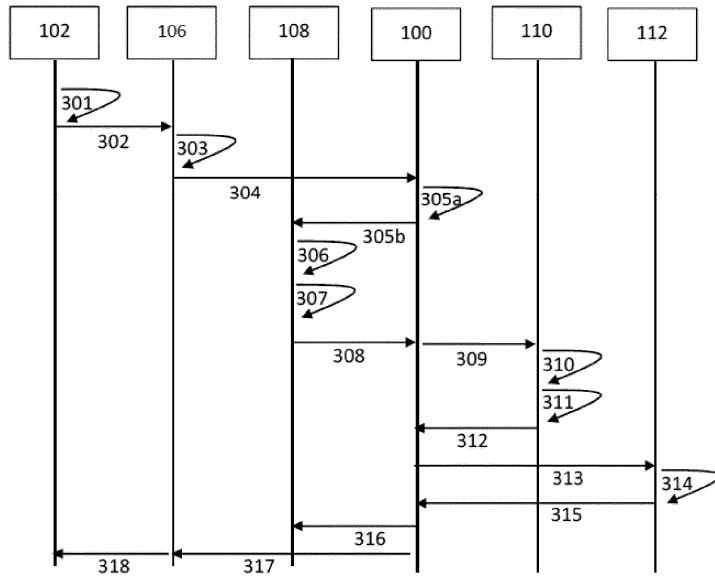
Фиг. 1



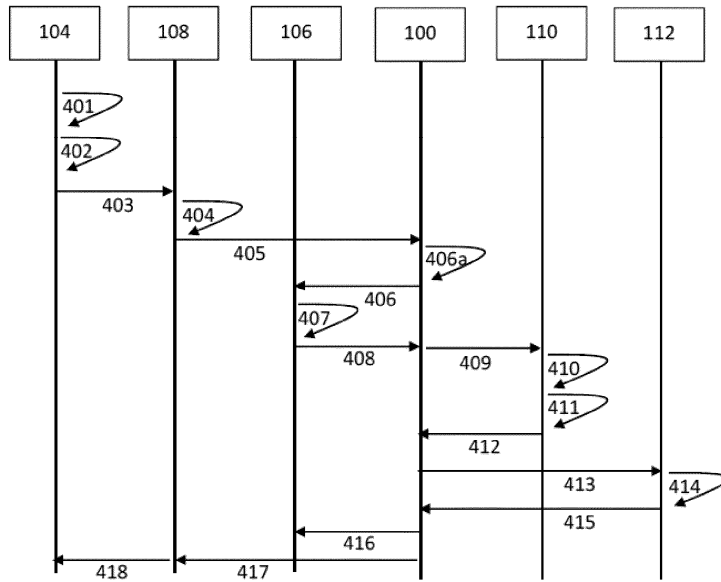
Фиг. 2а



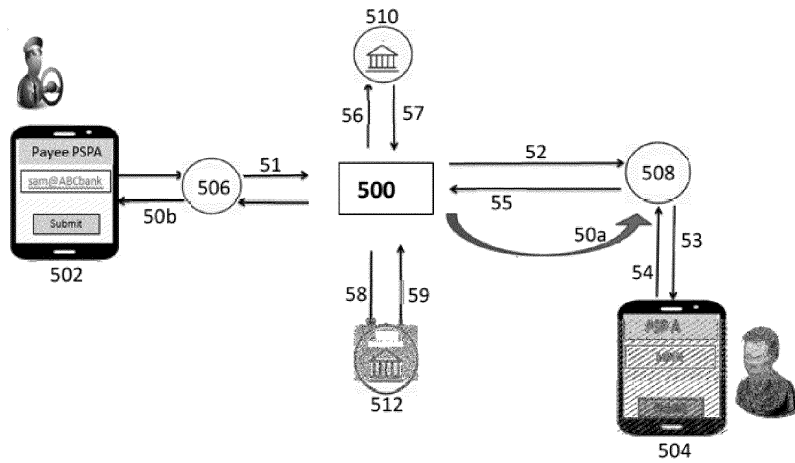
Фиг. 2b



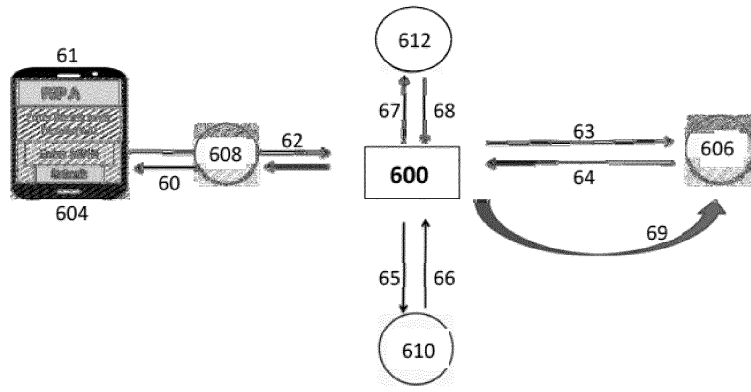
Фиг. 3



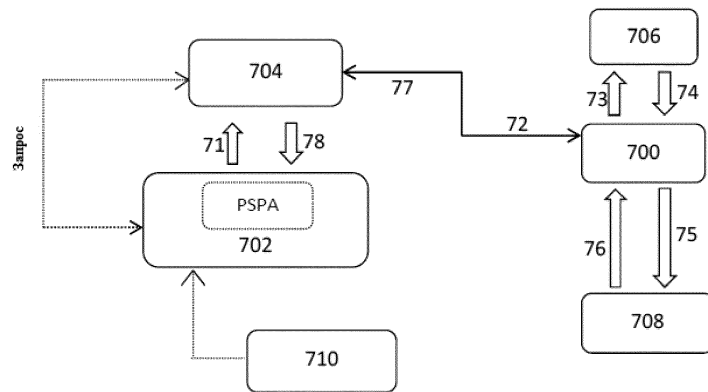
Фиг. 4



Фиг. 5



Фиг. 6



Фиг. 7