(19) Евразийское патентное ведомство

(21) 202393454 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2024.09.17

(22) Дата подачи заявки
2023.12.26

(51) Int. Cl. ***G06F 21/44*** (2013.01)
G06F 17/00 (2019.01)

(54) СПОСОБ И СИСТЕМА ПОДТВЕРЖДЕНИЯ ТРАНЗАКЦИЙ В МОБИЛЬНОМ ПРИЛОЖЕНИИ С ПОМОЩЬЮ ФОРМИРОВАНИЯ ОДНОРАЗОВЫХ СЕССИОННЫХ ИДЕНТИФИКАТОРОВ НА МОБИЛЬНОМ УСТРОЙСТВЕ ПОЛЬЗОВАТЕЛЯ ПОД УПРАВЛЕНИЕМ ОС ANDROID

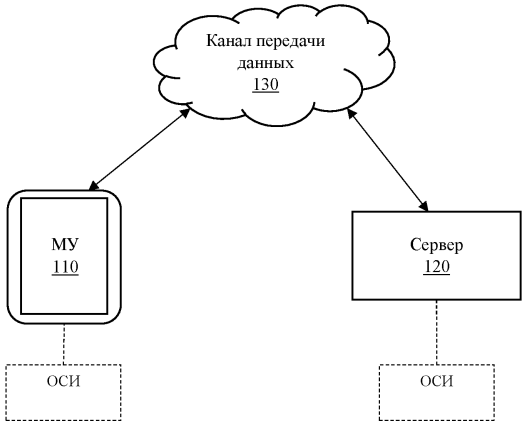
(31) **2023125437**
(32) **2023.10.04**
(33) **RU**

(71) Заявитель:
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК) (RU)

(72) Изобретатель:
Губанов Дмитрий Николаевич,
Широков Артём Александрович,
Нагорнов Иван Григорьевич (RU)

(74) Представитель:
Герасин Б.В. (RU)

(57) Изобретение относится к области компьютерной техники, в частности к методам защиты данных, а именно к методам подтверждения транзакций в мобильном приложении пользователя. Техническим результатом является повышение безопасности выполнения транзакций. Заявленное решение осуществляется с помощью способа подтверждения транзакций в мобильном приложении (МП) с помощью формирования одноразовых сессионных идентификаторов (ОСИ) на мобильном устройстве (МУ) пользователя под управлением ОС Android, содержащий этапы, на которых: a) получают запрос на совершение транзакции в МП на МУ пользователя; b) формируют запрос от МУ на сервер для получения списка параметров и алгоритма построения последовательности параметров для формирования ОСИ на МУ, при этом список параметров включает в себя следующие параметры МУ: параметры процессора, параметры камеры, параметры модуля памяти, параметры радиомодуля, системные параметры; c) принимают на МУ список параметров и алгоритм построения последовательности параметров; d) формируют на сервере ОСИ для МУ на основании данных, переданных на МУ на этапе c), и выполняют его запись в базу данных (БД) для соответствующего МУ; e) формируют на МУ ОСИ для МП на основании данных, полученных на этапе c), с помощью шифрования полученной последовательности параметров и алгоритма ее построения; f) отправляют сформированный на этапе e) ОСИ на сервер и осуществляют его дешифрование; g) выполняют сравнение полученного в ходе дешифрации ОСИ МП с ОСИ, хранящимся в БД; h) на основании сравнения ОСИ, выполненного на этапе g), одобряют или запрещают выполнение транзакции.



202393454 A1

202393454 A1

МПК: G06F 17/00; G06F 21/44

СПОСОБ И СИСТЕМА ПОДТВЕРЖДЕНИЯ ТРАНЗАКЦИЙ В МОБИЛЬНОМ ПРИЛОЖЕНИИ С ПОМОЩЬЮ ФОРМИРОВАНИЯ ОДНОРАЗОВЫХ СЕССИОННЫХ ИДЕНТИФИКАТОРОВ НА МОБИЛЬНОМ УСТРОЙСТВЕ ПОЛЬЗОВАТЕЛЯ ПОД УПРАВЛЕНИЕМ ОС ANDROID

ОБЛАСТЬ ТЕХНИКИ

[0001] Заявленное решение относится к области компьютерной техники, в частности к методам защиты данных, а именно к методам подтверждения транзакций в мобильном приложении пользователя.

УРОВЕНЬ ТЕХНИКИ

[0002] В настоящее время применение мобильных приложений для получения финансовых услуг является широко используемым способом взаимодействия пользователей с банками. Однако с массовым распространением получения услуг в цифровом формате возросло также и количество мошеннической активности, направленной на хищение средств пользователей, что обуславливает необходимость разработки новых средств защиты пользователей от действий мошенников.

[0003] Банковские мобильные приложения (далее - МП) используются клиентами банков для совершения различных операций (транзакций), а также для получения множества сервисов и услуг. При совершении данных манипуляций в МП банк может запрашивать у клиента дополнительное подтверждение совершаемых транзакций для их валидации, а иногда и для придания законной (юридической) силы тем событиям, которые последуют после выполнения транзакции, либо оказания услуги. Подтверждение операций может осуществляться по инициативе банка в целях противодействия финансовому мошенничеству, а также на основании требований регуляторных органов. В связи с этим валидация событий в банковском мобильном приложении имеет высокую значимость, а её некорректная работа может привести к сбоям в работе МП и нести значительные негативные последствия как для клиента, так и для банка.

[0004] К традиционным и широко применяемыми банками способами валидация можно отнести:

- SMS или PUSH сообщения, содержащие одноразовый код подтверждения (OTP);
- исходящий или входящий вызов из контактного центра банка с подтверждением у оператора банка, либо посредством IVR (Interactive Voice Response);

– личное посещение клиентом отделения банка.

[0005] Банковские приложения и клиенты банков подвергаются со стороны злоумышленников различным атакам для получения информации с OTP из SMS и PUSH сообщении, либо введении операторов контактных центров и других работников банков в заблуждение. Конечной целью данных атак злоумышленников является финансовое мошенничество и\или хищение денежных средств.

[0006] Использование любого из вышеописанных способов валидации транзакций имеет свои особенности и накладывает определённые ограничения на их применение. Так, например, валидация посредством SMS сообщений и голосовых вызовов в контактный центр несёт значительные затраты на содержание и для SMS имеет высокие риски со стороны операторов сотовой связи и возможности нелегитимной замены SIM карты абонента – клиента банка, совершённая злоумышленником. Подтверждение операций при личном посещении клиентом отделения банка оказывает негативное воздействие на лояльность клиентов и влечёт за собой снижение выручки банка и повышение нагрузки на операционных сотрудников отделений. Таким образом, исключительное использование любого из существующих способов валидации транзакций не представляется возможным.

[0007] Наиболее распространенным подходом в области подтверждения транзакций, совершаемых с помощью мобильных устройств, является применение двухфакторной верификации (2FA) по технологии 3D-Secure (https://ru.wikipedia.org/wiki/3-D_Secure).

[0008] Существенной проблемой существующих 2FA решений является то, что они генерируют случайный код, который может быть перехвачен злоумышленниками для совершения противоправных действий. Предлагаемое решение реализует новый более эффективный подход в части защиты транзакций, реализуемый с помощью генерирования одноразовых сессионных идентификаторов (ОСИ), формируемых на основании данных об аппаратных элементах мобильного устройства.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

[0009] Заявленное изобретение позволяет решить техническую проблему в части создания нового устойчивого одноразового сессионного идентификатора (ОСИ) МУ для подтверждения транзакций в мобильных приложениях.

[0010] Техническим результатом является повышение безопасности выполнения транзакций.

[0011] Заявленное решение осуществляется с помощью способа подтверждения транзакций в мобильном приложении (МП) с помощью формирования одноразовых

сессионных идентификаторов (ОСИ) на мобильном устройстве (МУ) пользователя под управлением ОС Android, содержащий этапы, на которых:

a) получают запрос на совершение транзакции в МП на МУ пользователя;
b) формируют запрос от МУ на сервер для получения списка параметров и алгоритма построения последовательности параметров для формирования ОСИ на МУ, при этом список параметров включает в себя следующие параметры МУ: параметры процессора, параметры камеры, параметры модуля памяти, параметры радиомодуля, системные параметры;
c) принимают на МУ список параметров и алгоритм построения последовательности параметров;
d) формируют на сервере ОСИ для МУ на сновании данных, переданных на МУ на этапе c), и выполняют его запись в базу данных (БД) для соответствующего МУ;
e) формируют на МУ ОСИ для МП на основании данных, полученных на этапе c), с помощью шифрования полученной последовательности параметров и алгоритма ее построения;
f) отправляют сформированный на этапе e) ОСИ на сервер и осуществляют его дешифрование;
g) выполняют сравнение полученного в ходе дешифрации ОСИ МП с ОСИ, хранящимся в БД;
h) на основании сравнения ОСИ, выполненного на этапе g), одобряют или запрещают выполнение транзакции.

[0012] В одном из частных примеров реализации алгоритм построения последовательности параметров представляет собой алгоритм рандомизации.

[0013] В другом частном примере реализации на этапе e) применяется алгоритм ассиметричного шифрования (RSA).

[0014] В другом частном примере реализации этапы b) – h) выполняются в заданный временной диапазон выполнения транзакции.

[0015] В другом частном примере реализации дополнительно формируют статичный идентификатор МУ с помощью сбора параметров МУ, включающих в себя: параметры процессора, параметры модуля камеры, параметры модуля памяти, параметры радиомодуля, и по меньшей мере данные марки мобильного устройства, и последующего хэширования полученного набора параметров.

[0016] В другом частном примере реализации статичный идентификатор создается на МУ пользователя, отправляется и проверяется на сервере при каждом запросе на совершение транзакции МУ.

[0017] В еще одном предпочтительном варианте осуществления изобретения заявлена система подтверждения транзакций в мобильном приложении (МП) с помощью формирования одноразовых сессионных идентификаторов (ОСИ) на мобильном устройстве (МУ) пользователя под управлением ОС Android, в которой:

МУ выполнено с возможностью получать запрос на совершение транзакции в МП на МУ пользователя;

формировать запрос от МУ на сервер для получения списка параметров и алгоритма построения последовательности параметров для формирования ОСИ на МУ, при этом список параметров включает в себя следующие параметры МУ: параметры процессора, параметры камеры, параметры модуля памяти, параметры радиомодуля, системные параметры;

принимать от сервера список параметров и алгоритм построения последовательности параметров;

формировать ОСИ для МП на основании данных, полученных от сервера, с помощью шифрования полученной последовательности параметров и алгоритма ее построения;

отправлять сформированный ОСИ на сервер;

сервер выполнен с возможностью формирования на сервере ОСИ для МУ на сновании данных, переданных на МУ в ответ на поступивший запрос, и выполняют его запись в базу данных (БД) для соответствующего МУ;

дешифровки сформированного ОСИ МП, получаемого от МУ;

сравнения полученного в ходе дешифрации ОСИ МП с ОСИ, хранящимся в БД;

на основании сравнения ОСИ, осуществлять одобрение или запрет выполнения транзакции.

[0018] В одном из частных примеров реализации построение последовательности параметров представляет собой алгоритм рандомизации.

[0019] В другом частном примере реализации шифрование осуществляется с помощью алгоритма ассиметричного шифрования (RSA).

[0020] В другом частном примере реализации дополнительно формируют статичный идентификатор МУ с помощью сбора параметров МУ, включающих в себя: параметры процессора, параметры модуля камеры, параметры модуля памяти, параметры радиомодуля, и по меньшей мере данные марки мобильного устройства, и последующего хэширования полученного набора параметров.

[0021] В другом частном примере реализации статичный идентификатор создается на МУ пользователя, отправляется и проверяется на сервере при каждом запросе на совершение транзакции МУ.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0022] Фиг. 1 иллюстрирует общую схему работы решения.

[0023] Фиг. 2 иллюстрирует блок-схему реализации заявленного способа.

[0024] Фиг. 3 иллюстрирует схему вычислительного устройства.

ОСУЩЕСТВЛЕНИЕ ИЗОБРЕТЕНИЯ

[0025] На Фиг. 1 представлен общий вид схемы реализации заявленного решения, которое включает в себя МУ пользователя (110), соединенный каналом передачи данных (130) с сервером (120), выполняющим обработку данных через API. В качестве МУ (110) может применяться смартфон, фаблет или планшет под управление ОС Android, на котором установлено МП (например, Сбербанк Онлайн). В части канала передачи данных (130) применяется сеть «Интернет», обеспечивая обмен данными между МУ (110) и сервером (120).

[0026] На Фиг. 2 представлена блок-схема выполнения этапов способа (200) подтверждения транзакций в МП. После установки платежного МП (201), например, Сбербанк Онлайн, программная логика приложения запрашивает данные для последующей регистрации пользователя. Такими данными могут являться, ФИО, паспортные данные, номер платежной карты, номер телефона, логин/пароль для входа в приложение и т.п. Дополнительно может применяться биометрическая информация. После успешной регистрации для каждого пользователя создается уникальная запись под соответствующим идентификатором, которая сохраняется на сервере в единой базе данных (БД).

[0027] После регистрации в приложении на этапе (202), клиентская часть МП фиксирует вход в МП. При инициировании выполнения транзакции пользователем МП на МУ (110) формируется запрос на сервер (120) для получения списка параметров и алгоритма формирования последовательности параметров, с помощью которых будет формироваться ОСИ для МП. Список параметров включает в себя следующие параметры МУ: параметры процессора, параметры камеры, параметры модуля памяти, параметры радиомодуля, системные параметры. Сервер (120) осуществляет запрос параметров и алгоритма формирования их последовательности в БД и передает их на МУ (110).

[0028] Сбор параметров осуществляется посредством программной логики платежного МП, имеющего доступ к ОС мобильного устройства. В рамках осуществления настоящего этапа осуществляется сбор следующих параметров: параметры процессора, параметры модуля камеры, параметры модуля памяти, параметры радиомодуля, и по меньшей мере данные марки мобильного устройства.

[0029] Данные мобильного устройства собираются по основным аппаратным модулям (процессор, память, камера, радиомодуль), а также системные данные, идентифицирующие само устройство.

[0030] Параметры процессора могут выбираться из следующих данных, представленных в Таблице 1.

Таблица 1. Параметры процессора

CPU_CORES	Количество ядер процессора
CPU_MHZ	Частота процессора
MODEL_NAME	Модель процессора
CPU_FAMILY	Название семейства процессора
KERNEL_OS_NAME	Название ядра
KERNEL_OS_ARCH	Архитектура ядра
CPU_ABI	Поддерживаемая архитектура
CPU_ABI2	Поддерживаемая архитектура

[0031] Пример используемых параметров модуля камеры приведены в Таблице 2.

Таблица 2. Параметры камеры

CAMERA_SENSOR_SIZE	Размер сенсора камеры
CAMERA_0_FOCAL_LENGTH	Фокальное расстояние камеры
CAMERA_0_HORIZONTAL_ANGLE	Горизонтальный угол отстройки камеры
CAMERA_0_VERTICAL_ANGLE	Вертикальный угол отстройки камеры
MAX_FRAME_DURATION	Максимальная продолжительность кадра

[0032] Параметры модуля памяти могут включать в себя параметры, указанные в Таблице 3.

Таблица 3. Параметры модуля памяти

MEMTOTAL	Общий объем физической оперативной памяти
SWAPTOTAL	Общий объем доступного свопа («Своп» - файл\раздел подкачки операционной системы предназначенный для повышения быстродействия и оптимизации использования приложений на мобильном устройстве).
VMALLOCTOTAL	Общий объем памяти от общего выделенного виртуального адресного пространства

[0033] Пример используемых параметров радиомодуля приведен в Таблице 4.

Таблица 4. Параметры радиомодуля

WIDEVINE_UUID_SYSTEM_ID	Идентификатор DRM-схемы
RADIO_VERSION	Версия прошивки радио модуля
HARDWARE	Название оборудования (из командной строки ядра)
BOARD	Название базовой платы

[0034] Также дополнительно для формирования идентификатора используются системные параметры, приведенные в Таблице 5.

Таблица 5. Системные параметры

BOGOMIPS	Параметр проверки диапазона процессора
OUTPUT_SIZES	Разрешение экрана
MANUFACTURER	Название производителя
MODEL	Название мобильного устройства, видимое пользователю устройства
DEVICE	Название промышленного образца (заводское наименование марки и модельного ряда мобильных устройств)
ID	Номер списка изменений, либо метка типа «M4-rc20»
DISPLAY	Строка идентификатора сборки
BRAND	Название бренда производителя устройства

[0035] Далее на этапе (203) после того как сервер (120) передал параметры на МУ (110), на сервере (120) происходит формирование ОСИ для МУ (110). Алгоритм формирования последовательности из 28 вышеуказанных параметров представляет собой рандомизатор последовательности полученных сервером (120) параметров, за счёт чего количество возможных комбинаций для набора одного МУ (110) превышает 38 млн значений.

[0036] По факту сбора требуемого набора вышеуказанных параметров, на этапе (204) осуществляется их последующее хэширование с учетом выбранного алгоритма

рандомизации, переданного сервером (120). В качестве алгоритма рандомизации может применяться алгоритм Randomized Quick Sort или иной. ОС Android позволяет получать данные параметры без дополнительных разрешений со стороны владельца мобильного устройства.

[0037] В зависимости от типа решаемых задач идентификатор, получаемый на вышеописанных параметрах, является статическим , что достигается за счёт использования различных алгоритмов преобразования данных. При формировании ОСИ на МУ (110) применяется алгоритмов асимметричного шифрования (RSA) для повышения защищённости и повышения устойчивости соединения к различным векторам атак на банковскую инфраструктуру.

[0038] На этапе (204) по итогу применения функций хэширования формируется ОСИ, который может иметь следующий вид:
Wj6tqLi34kZsbPZCi+gGTyrTaHmoAn1jO1wMwAxSx0Wn:C3+zD3sl0XsjJOc:C3FzD3sl0XsjJOcWj6tqLi34kZsbPZCi+gGTyrTaHmoAn1jO1wlCY0Sx0Wn:C1fpwOcWj68LioBPZCiqyrGGJn1fVxv.

[0039] Зашифрованный ОСИ передается на сервер (120) где впоследствии на этапе (205) дешифруется для целей проверки его совпадения с ОСИ, который был сформирован на этапе (203), хранящегося в БД. На этапе (206) в случае если ОСИ совпадают, то транзакция, совершаемая в МП, одобряется. В противном случае транзакция отклоняется. Проверка ОСИ, формируемого на МУ (110) и сервере (120) выполняется автоматически и не требует от пользователя МУ (110) дополнительного ввода или действий, что дополнительно повышает безопасность данной операции и снижает риск перехвата ОСИ. Как правило, время для проверки факта одобрения транзакции имеет установленный диапазон, например, 30 сек, 1 минута и т.п. Диапазон может варьироваться. Проверка ОСИ осуществляется в рамках вышеупомянутого установленного диапазона.

[0040] Дополнительно для МУ (110) может формироваться статичный идентификатор способом, который был описан в патенте №2772571 (ПАО Сбербанк, 08.09.2022), который сохраняется в БД сервера (120) и может применяться для дополнительной аутентификации МУ (110).

[0041] Уникальность подхода заключается в формировании ОСИ именно на клиентской части приложения по той логике, которую ему передаёт серверная часть, на данных, которые известны только клиентской и серверной части. Данный подход значительно повышает уровень доверия (при тождественности идентификаторов) клиент-серверному взаимодействию и при этом сохраняется высокий уровень быстродействия взаимодействия в целом. При достаточной защите исходного кода от злоумышленников,

самостоятельно (несанкционированно) сгенерировать ОСИ в модифицированном мобильном приложении не представляется возможным.

[0042] Применимость подхода имеет разные прикладные стороны, это как уже описанный выше метод использования идентификатора в системах, осуществляющих мониторинг и блокировку подозрительных транзакций, так и системы, осуществляющие авторизацию клиентов и устройств.

[0043] На Фиг. 3 представлен общий вид вычислительного устройства (300), с помощью которого может быть реализовано заявленное решение. В общем случае, вычислительное устройство (300) содержит объединенные общей шиной информационного обмена один или несколько процессоров (301), средства памяти, такие как ОЗУ (302) и ПЗУ (303), интерфейсы ввода/вывода (304), устройства ввода/вывода (305), и устройство для сетевого взаимодействия (306).

[0044] Процессор (301) (или несколько процессоров, многоядерный процессор) могут выбираться из ассортимента устройств, широко применяемых в текущее время, например, компаний Intel™, AMD™, Apple™, Samsung Exynos™, MediaTEK™, Qualcomm Snapdragon™ и т.п. Под процессором также необходимо учитывать графический процессор, например, GPU NVIDIA или ATI, который также является пригодным для полного или частичного выполнения способа (200). При этом, средством памяти может выступать доступный объем памяти графической карты или графического процессора.

[0045] ОЗУ (302) представляет собой оперативную память и предназначено для хранения исполняемых процессором (301) машиночитаемых инструкций для выполнение необходимых операций по логической обработке данных. ОЗУ (302), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.).

[0046] ПЗУ (303) представляет собой одно или более устройств постоянного хранения данных, например, жесткий диск (HDD), твердотельный накопитель данных (SSD), флэш-память (EEPROM, NAND и т.п.), оптические носители информации (CD-R/RW, DVD-R/RW, BlueRay Disc, MD) и др.

[0047] Для организации работы компонентов устройства (300) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (304). Выбор соответствующих интерфейсов зависит от конкретного исполнения вычислительного устройства, которые могут представлять собой, не ограничиваясь: PCI, AGP, PS/2, IrDa, FireWire, LPT, COM, SATA, IDE, Lightning, USB (2.0, 3.0, 3.1, micro, mini, type C), TRS/Audio jack (2.5, 3.5, 6.35), HDMI, DVI, VGA, Display Port, RJ45, RS232 и т.п.

[0048] Для обеспечения взаимодействия пользователя с вычислительным устройством (400) применяются различные средства (305) В/В информации, например, клавиатура, дисплей (монитор), сенсорный дисплей, тач-пад, джойстик, манипулятор мышь, световое перо, стилус, сенсорная панель, трекбол, динамики, микрофон, средства дополненной реальности, оптические сенсоры, планшет, световые индикаторы, проектор, камера, средства биометрической идентификации (сканер сетчатки глаза, сканер отпечатков пальцев, модуль распознавания голоса) и т.п.

[0049] Средство сетевого взаимодействия (306) обеспечивает передачу данных устройством (300) посредством внутренней или внешней вычислительной сети, например, Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (306) может использоваться, но не ограничиваться: Ethernet карта, GSM модем, GPRS модем, LTE модем, 5G модем, модуль спутниковой связи, NFC модуль, Bluetooth и/или BLE модуль, Wi-Fi модуль и др.

[0050] Дополнительно могут применяться также средства спутниковой навигации в составе устройства (300), например, GPS, ГЛОНАСС, BeiDou, Galileo.

[0051] Представленные материалы заявки раскрывают предпочтительные примеры реализации технического решения и не должны трактоваться как ограничивающие иные, частные примеры его воплощения, не выходящие за пределы испрашиваемой правовой охраны, которые являются очевидными для специалистов соответствующей области техники.

ФОРМУЛА

1. Способ подтверждения транзакций в мобильном приложении (МП) с помощью формирования одноразовых сессионных идентификаторов (ОСИ) на мобильном устройстве (МУ) пользователя под управлением ОС Android, содержащий этапы, на которых:

a) получают запрос на совершение транзакции в МП на МУ пользователя;

b) формируют запрос от МУ на сервер для получения списка параметров и алгоритма построения последовательности параметров для формирования ОСИ на МУ, при этом список параметров включает в себя следующие параметры МУ: параметры процессора, параметры камеры, параметры модуля памяти, параметры радиомодуля, системные параметры;

c) принимают на МУ список параметров и алгоритм построения последовательности параметров;

d) формируют на сервере ОСИ для МУ на сновании данных, переданных на МУ на этапе c), и выполняют его запись в базу данных (БД) для соответствующего МУ;

e) формируют на МУ ОСИ для МП на основании данных, полученных на этапе c), с помощью шифрования полученной последовательности параметров и алгоритма ее построения;

f) отправляют сформированный на этапе e) ОСИ на сервер и осуществляют его дешифрование;

g) выполняют сравнение полученного в ходе дешифрации ОСИ МП с ОСИ, хранящимся в БД;

h) на основании сравнения ОСИ, выполненного на этапе g), одобряют или запрещают выполнение транзакции.

2. Способ по п.1, в котором алгоритм построения последовательности параметров представляет собой алгоритм рандомизации.

3. Способ по п.1, в котором на этапе e) применяется алгоритм ассиметричного шифрования (RSA).

4. Способ по п.1, в котором этапы b) – h) выполняются в заданный временной диапазон выполнения транзакции.

5. Способ по п.1, в котором дополнительно формируют статичный идентификатор МУ с помощью сбора параметров МУ, включающих в себя: параметры процессора, параметры модуля камеры, параметры модуля памяти, параметры радиомодуля, и по

меньшей мере данные марки мобильного устройства, и последующего хэширования полученного набора параметров.

6. Способ по п.5, в котором статичный идентификатор создается на МУ пользователя, отправляется и проверяется на сервере при каждом запросе на совершение транзакции МУ.

7. Система подтверждения транзакций в мобильном приложении (МП) с помощью формирования одноразовых сессионных идентификаторов (ОСИ) на мобильном устройстве (МУ) пользователя под управлением ОС Android, в которой:

МУ выполнено с возможностью

получать запрос на совершение транзакции в МП на МУ пользователя;

формировать запрос от МУ на сервер для получения списка параметров и алгоритма построения последовательности параметров для формирования ОСИ на МУ, при этом список параметров включает в себя следующие параметры МУ: параметры процессора, параметры камеры, параметры модуля памяти, параметры радиомодуля, системные параметры;

принимать от сервера список параметров и алгоритм построения последовательности параметров;

формировать ОСИ для МП на основании данных, полученных от сервера, с помощью шифрования полученной последовательности параметров и алгоритма ее построения;

отправлять сформированный ОСИ на сервер;

сервер выполнен с возможностью

формирования на сервере ОСИ для МУ на сновании данных, переданных на МУ в ответ на поступивший запрос, и выполняют его запись в базу данных (БД) для соответствующего МУ;

дешифровки сформированного ОСИ МП, получаемого от МУ;

сравнения полученного в ходе дешифрации ОСИ МП с ОСИ, хранящимся в БД;

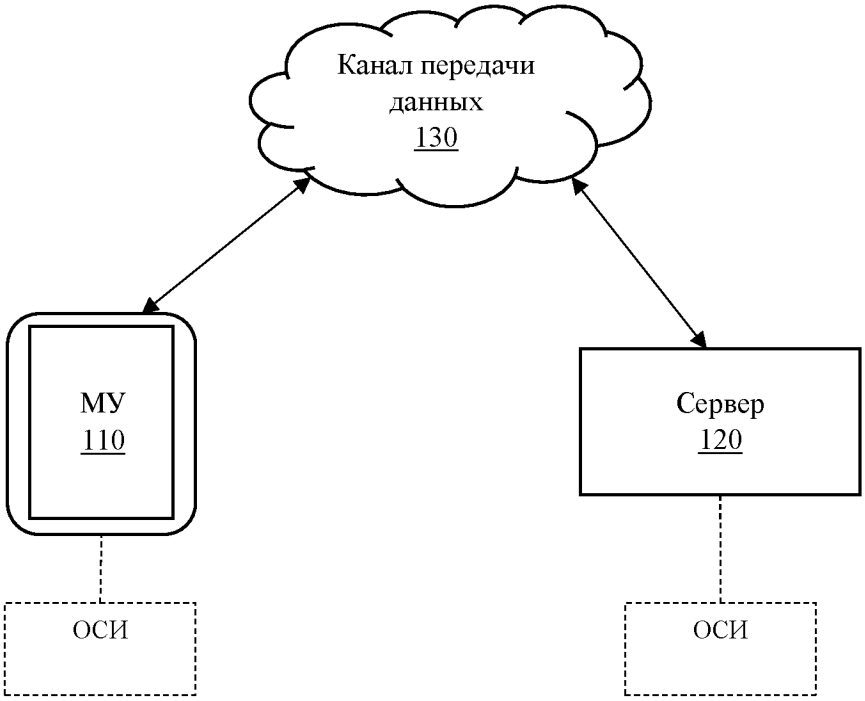
на основании сравнения ОСИ, осуществлять одобрение или запрет выполнения транзакции.

8. Система по п.7, в которой построение последовательности параметров представляет собой алгоритм рандомизации.

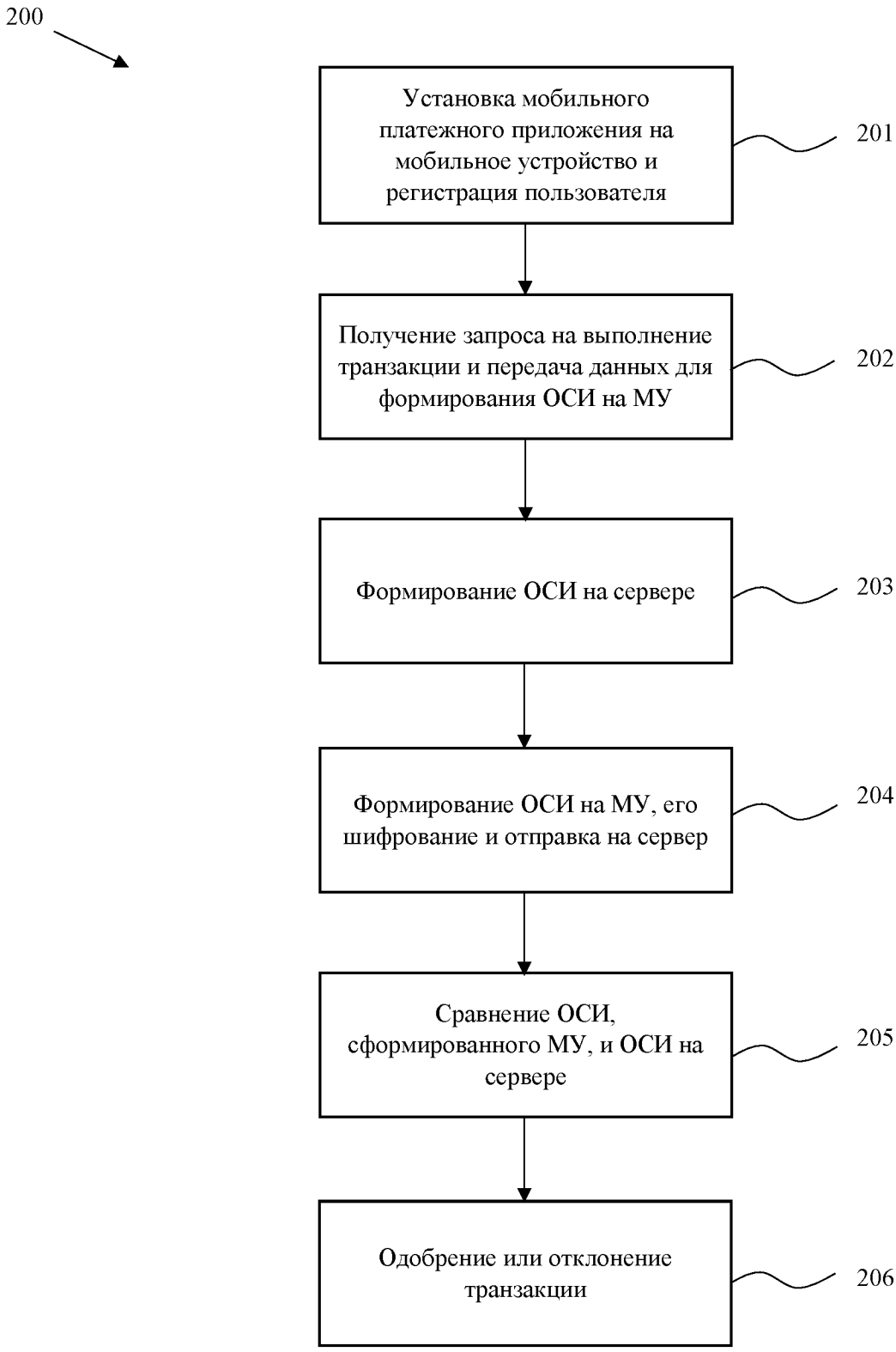
9. Система по п.7, в которой шифрование осуществляется с помощью алгоритма ассиметричного шифрования (RSA).

10. Система по п.7, в которой дополнительно формируют статичный идентификатор МУ с помощью сбора параметров МУ, включающих в себя: параметры процессора, параметры модуля камеры, параметры модуля памяти, параметры радиомодуля, и по меньшей мере данные марки мобильного устройства, и последующего хэширования полученного набора параметров.

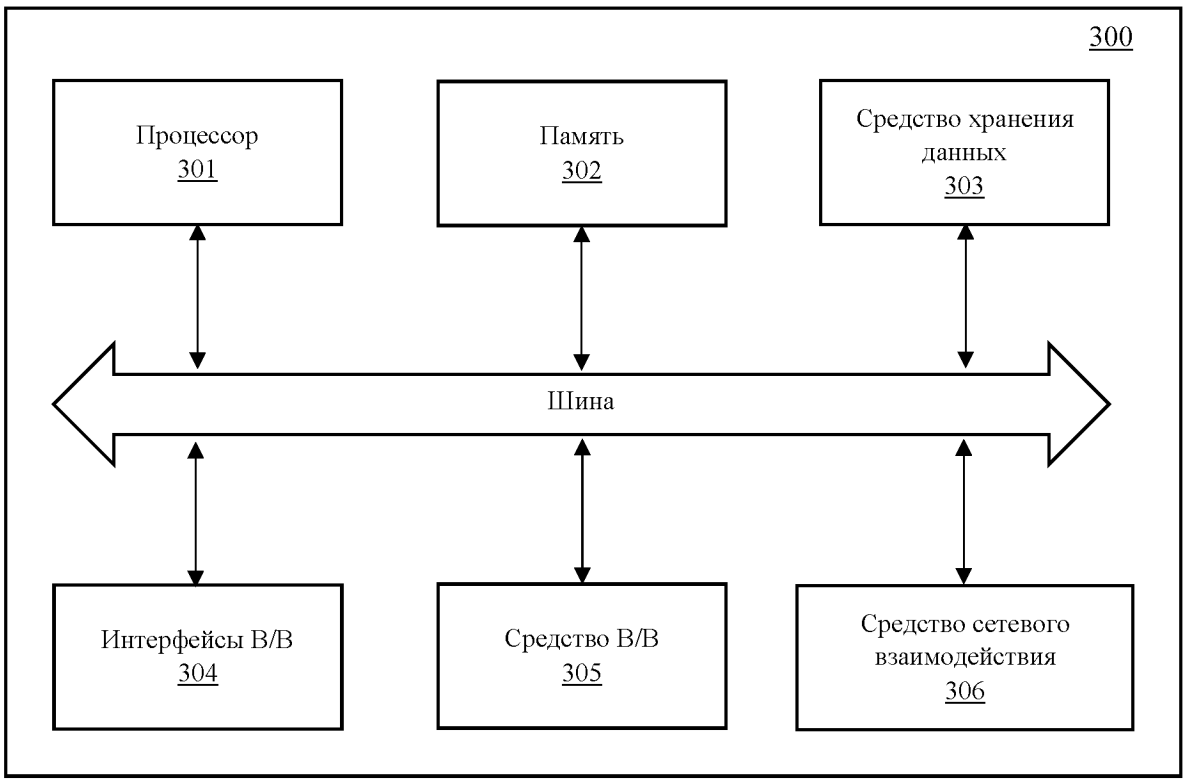
11. Система по п.10, в которой статичный идентификатор создается на МУ пользователя, отправляется и проверяется на сервере при каждом запросе на совершение транзакции МУ.



Фиг. 1


200
Установка мобильного платежного приложения на мобильное устройство и регистрация пользователя
201
Получение запроса на выполнение транзакции и передача данных для формирования ОСИ на МУ
202
Формирование ОСИ на сервере
203
Формирование ОСИ на МУ, его шифрование и отправка на сервер
204
Сравнение ОСИ, сформированного МУ, и ОСИ на сервере
205
Одобрение или отклонение транзакции
206

Фиг. 2


300
Процессор
301
Память
302
Средство хранения данных
303
Шина
Интерфейсы В/В
304
Средство В/В
305
Средство сетевого взаимодействия
306

Фиг. 3

ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ

(статья 15(3) ЕАПК и правило 42 Патентной инструкции к ЕАПК)

Номер евразийской заявки:

202393454

А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:

МПК:		СПК:
G06F 21/44	(2013.01)	**G06F 21/44**
G06F 17/00	(2019.01)	**G06F 17/00**

Б. ОБЛАСТЬ ПОИСКА:

G06F 21/00-21/44, G06F 15/00-15/16, 17/00 -17/30, G06Q 20/00-20/38

Электронная база данных, использовавшаяся при поиске (название базы и, если возможно, используемые поисковые термины)
Espacenet, EAPATIS, PAJ, WIPO, GOOGLE, K-PION, «ПОИСКОВАЯ ПЛАТФОРМА» (РОСПАТЕНТ)

В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
A	RU 2796211 C1, (ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК)), 2023-05-17	1-11
A	RU 2779521 C1, (ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ")), 2022-09-08	1-11
A	US 2022/0207523 A1, (VISA INTERNATIONAL SERVICE ASSOCIATION), 2022-06-30	1-11
A	US 2011/0321146 A1, (VERNOM J. et al), 2011-12-29	1-11

☐ последующие документы указаны в продолжении графы

* Особые категории ссылочных документов:
«A» - документ, определяющий общий уровень техники
«D» - документ, приведенный в евразийской заявке
«E» - более ранний документ, но опубликованный на дату подачи евразийской заявки или после нее
«O» - документ, относящийся к устному раскрытию, экспонированию и т.д.
"P" - документ, опубликованный до даты подачи евразийской заявки, но после даты испрашиваемого приоритета"
«T» - более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения
«X» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну или изобретательский уровень, взятый в отдельности
«Y» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий изобретательский уровень в сочетании с другими документами той же категории
«&» - документ, являющийся патентом-аналогом
«L» - документ, приведенный в других целях

Дата проведения патентного поиска: 10 июня 2024 (10.06.2024)

Документ подписан электронной подписью
Сертификат: 1711998581100
Владелец: CN=Аверкиев С.
Действителен: 01.04.2024-01.04.2025

Уполномоченное лицо:
Начальник Управления экспертизы С.Е. Аверкиев