(19) Евразийское патентное ведомство

(11) 033637 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2019.11.12

(21) Номер заявки
201700611

(22) Дата подачи заявки
2017.12.27

(51) Int. Cl. ***G06Q 20/20*** (2012.01)
G06Q 20/40 (2012.01)

(54) СИСТЕМА УПРАВЛЕНИЯ POS-ТЕРМИНАЛЬНОЙ СЕТИ

(31) **2017145128**
(32) **2017.12.21**
(33) **RU**
(43) **2019.06.28**

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

(72) Изобретатель:
Брик Алексей Владимирович, Нещадимов Юрий Анатольевич (RU)

(74) Представитель:
Астафьева С.А., Герасин Б.В. (RU)

(56) US-A1-20080283592
US-A1-20140214576
US-A1-20160292660
WO-A1-2015187907
US-A1-20050257205
US-B2-7889384

(57) Техническое решение, в общем, относится к области вычислительной техники, в частности к системе для управления POS-терминальной сети. Техническим результатом является обеспечение централизованного управления POS-терминалами под управлением стандарта UPOS с реализацией функций обновления программной составляющей множества POS-терминалов. Заявленный технический результат достигается за счет системы управления POS-терминальной сети, которая содержит по меньшей мере один UPOS-сервер, объединенный каналом передачи данных с устройством осуществления финансовых транзакций, к которому подключен один или более POS-терминалов, осуществляющих функционирование посредством ПО UPOS, модуль UPOS-агента и сервер авторизации транзакций, в которой модуль UPOS-агента выполнен с возможностью обеспечения маршрутизации данных между UPOS-сервером, POS-терминалами и устройством осуществления транзакций; POS-терминал выполнен с возможностью приема клиентских запросов на выполнение транзакций, верификации клиентов, шифрования транзакционных данных клиентских запросов; UPOS-сервер выполнен с возможностью мониторинга и контроля параметров POS-терминалов, управления работой POS-терминала, генерирования сценариев обработки транзакций и обмена данными с сервером авторизации транзакций, обновления параметров POS-терминала.

033637 B1

033637 B1

Область техники

Настоящее техническое решение, в общем, относится к области вычислительной техники, в частности к системе для управления POS-терминальной сети.

Уровень техники

Из уровня техники известно решение по эффективному управлению POS-терминалами с помощью универсального протокола обмена сообщениями Unified POS (UPOS) (US 7889384, опубликовано 15.02.2011, патентообладатель: IBM Corporation), которое раскрывает механизм организации команд, передаваемых от устройства кассира на POS-терминал при выполнении транзакций. В частности, данное решение направлено на снижение информации, печатаемой с помощью принтера POS-терминала при распознавании сложных транзакционных операций, что существенно увеличивает время обработки и может привести к потере части или всей информации, идентифицирующей транзакцию.

Одним из примеров решения указанной проблемы, предлагаемых в вышеуказанном патенте, является перенос части функционала, исполняемого программной логикой POS-терминала, на хост, к которому он подключен, для обработки на основании идентификаторов соответствующих операций программными средствами хоста, что позволит снизить вычислительную нагрузку и шанс возникновения ошибок в распознавании и обработке параметров транзакций.

Существенным недостатком данного решения является конфигурация системы выполнения транзакций, поскольку перенос части функционала на хост решает частично проблему снижения вычислительной нагрузки и повышения стабильности работы POS-терминалов, но не позволяет избежать проблемы по управлению техническим состоянием терминалов.

Также существующая система регистрации и управления сетью POS-терминалов не позволяет оперативно обновлять ПО UPOS на всем терминальном парке с помощью единого узла, генерирующего соответствующие информационные команды.

На сегодняшний день обновление программного обеспечения приводит к большому количеству ошибок при тиражировании версий ПО. Вследствие этого на многих терминалах работают устаревшие версии ПО, что приводит к повышению времени обработки транзакций, несовместимости выполнения функционала и т.п. Кроме того, процедура обновления программного обеспечения и настроек часто приводит к нарушению работоспособности терминалов. В то же время развитие функциональности эквайринга требует регулярного оперативного обновления ПО терминалов.

Программное обеспечение UPOS развивалось эволюционным путем в течение многих лет. За это время в ПО накопилось большое количество доработок, которые накладывались друг на друга, что снижает читаемость текстов программ и, как следствие, отрицательно сказывается на возможности внесения изменений, а также увеличивает количество ошибок, возникающих в процессе внесения изменений.

Наличие в коде ПО UPOS как функций работы с устройствами POS-терминалов, так и бизнес логики приводит к увеличенному потреблению ресурсов терминала (процессор, оперативная и долговременная память), что приводит к повышенным требованиям к технической конфигурации терминалов.

Раскрытие изобретения

Технической проблемой, решаемой с помощью заявленного решения, является устранение существующих недостатков в части централизованного управления POS-терминалами с одновременным снижением вычислительной нагрузки при обработке транзакций.

Техническим результатом является обеспечение централизованного управления POS-терминалами под управлением стандарта UPOS с реализацией функций обновления программной составляющей множества POS-терминалов.

Дополнительным техническим результатом является снижение вычислительной нагрузки при обработке транзакций за счет переноса части функционала POS-терминала на UPOS-сервер и использование UPOS-агента на устройстве кассира, к которому подключен POS-терминал, выполняющий транзакции.

Заявленный технический результат достигается за счет системы управления POS-терминальной сети, которая содержит по меньшей мере один UPOS-сервер, объединенный каналом передачи данных с устройством осуществления финансовых транзакций, к которому подключен один или более POS-терминалов, осуществляющих функционирование посредством ПО UPOS, модуль UPOS-агента и сервер авторизации транзакций, в которой

модуль UPOS-агента выполнен с возможностью обеспечении маршрутизации данных между UPOS-сервером, POS-терминалами и устройством осуществления транзакций;

POS-терминал выполнен с возможностью приема клиентских запросов на выполнение транзакций, верификации клиентов, шифрования транзакционных данных клиентских запросов;

UPOS-сервер выполнен с возможностью мониторинга и контроля параметров POS-терминалов, управления работой POS-терминала, генерирования сценариев обработки транзакций и обмена данными с сервером авторизации транзакций, обновления параметров POS-терминала.

В частном варианте реализации системы модуль UPOS-агента реализует генерирование интерфейса обработки транзакций с помощью устройства осуществления финансовых транзакций.

В частном варианте реализации системы UPOS-агент и связанные с ним POS-терминалы связаны посредством локального сетевого соединения или посредством вычислительной сети.

В частном варианте реализации системы локальное соединение выбирается из групп: RS-232, USB, ЛВС или их сочетания.

В частном варианте реализации системы вычислительная сеть обеспечивает соединение посредством TCP/IP протокола.

В частном варианте реализации системы соединение осуществляется за счет устройства сетевой передачи данных POS-терминала, которое выбирается из группы: GPRS-модем, GSM-модем, 4C-модем, Wi-Fi адаптер, Ethernet-адаптер.

В частном варианте реализации системы UPOS-сервер дополнительно выполнен с возможностью опроса подключенных к нему POS-терминалов и сбора общего хеш-значения локального набора файлов по каждому терминалу.

В частном варианте реализации системы сервер осуществляет сравнение полученного хеш-значения каждого POS-терминала с эталонным значением, хранящимся на сервере. В частном варианте реализации системы в ходе сравнения сервер определяет по меньшей мере один файл из каждого хеш-значения POS-терминала, который не соответствует эталонному значению.

В частном варианте реализации системы в ответ на выявление расхождения в хеш-значении сервер передает эталонную версию файла на POS-терминал.

В частном варианте реализации системы UPOS-сервер содержит модуль настройки параметров POS-терминалов. В частном варианте реализации системы UPOS-сервер содержит модуль обработки правил взаимодействия с банковскими картами.

В частном варианте реализации системы UPOS-сервер содержит модуль формирования финансовых отчислений, выполненный с возможностью генерирования в ответ на обработку транзакций посредством POS-терминалов дополнительных финансовых движений по счету клиента.

В частном варианте реализации системы дополнительные финансовые движения выбираются из группы: скидки, учет бонусных средств на счете клиента, возврат части затраченной суммы оплаты или их сочетания.

В частном варианте реализации системы UPOS-сервер содержит модуль генерирования чеков.

Краткое описание чертежей

Фиг. 1 иллюстрирует общий вид заявленной системы.

Фиг. 2 иллюстрирует схему модулей POS-терминала и UPOS-агента.

Фиг. 3 иллюстрирует схему модулей UPOS-сервера.

Фиг. 4 иллюстрирует пример работы криптомодуля POS-терминала.

Фиг. 5 и 6 иллюстрируют пример шифрования данных.

Фиг. 7 и 8 иллюстрируют блок-схему выполнения транзакции.

Фиг. 9 иллюстрирует схему вычислительного устройства.

Осуществление изобретения

В настоящих материалах заявки будут использованы следующие термины и обозначения:

EMV (Europay+MasterCard+VISA) - международный стандарт для операций по банковским картам с чипом.

POS-терминал (торговый терминал) - электронное устройство, устанавливаемое рядом с кассовым аппаратом торгово-сервисного предприятия и позволяющее считывать информацию с магнитной полосы или чипа карточки и осуществлять связь с банком для проведения авторизации с целью осуществления операции по банковской карточке. Могут быть использованы для расчетов с использованием как магнитных карт, так и микропроцессорных.

CVM или CVM-лист (Cardholder Verification Method) - информация банка эмитента карты, записанная на EVM-чип карты.

UnifiedPOS (UPOS) - универсальный стандарт управления интерфейсами POS-терминалами, который обеспечивает единый программный интерфейс управления для POS-терминалов различных производителей.

UPOS-агент - программный модуль, установленный на устройстве для выполнения транзакций, обеспечивающий, по меньшей мере, маршрутизацию данных между POS-терминалом и управляющим сервером.

ПО - программное обеспечение.

Устройство выполнения транзакций - компьютерное устройство кассира с подключенным UPOS-агентом. В качестве устройства выполнения транзакций может применятся кассовое оборудование с операционной системой (например, Windows Embedded) или устройство на базе персонального компьютера.

Как представлено на фиг. 1, в общем виде заявленная система управления POS-терминальной сети содержит совокупность устройств, таких как POS-терминал (100), UPOS-агент (200), соединенный с процессором (250) устройства выполнения транзакций (300), UPOS-сервер (400) и сервер авторизации транзакций (500).

На фиг. 2 представлена схема модулей, входящих в состав POS-терминала (100) и UPOS-агента (200). POS-терминалы (100) обеспечивают работу с картами оплаты клиентов для осуществления процесса транзакции.

POS-терминал (100) содержит модуль верификации (101), который обеспечивает верификацию клиента на основании данных карты, с помощью которой выполняется процесс транзакции. Модуль (102) обеспечивает считывание параметров карты и передает их по универсальной шине в модуль (101). Карты оплаты могут выполняться с магнитной полосой или чипом.

Модуль хранения ключей (103) обеспечивает хранение ключей в защищенной области памяти POS-терминала, а также обеспечивает реализацию интерфейса управления ключами в незащищенной области памяти.

Модуль EMV (104) обеспечивает обработку транзакционных данных в соответствии со стандартом EMV при обработке данных по картам оплаты, снабженным чипом.

Модуль шифрования (105) обеспечивает шифрование данных терминала (100), ПИН-пада (109) и данных для передачи на сервер (400). Модуль (105) также выполняет расшифровку данных, получаемых от UPOS-сервера (400).

Модуль печати чеков (106) выполняет вывод чека на встроенный в терминал (100) принтер.

Модуль (107) интерфейса обеспечивает взаимодействие с клиентом терминала (100) с помощью генерирования отображения на дисплее терминала (110) требуемой информации по осуществления процесса транзакции.

Как указывалось выше, функционал терминала (100) содержит только базовые функции, которые позволяют осуществить сбор первичной информации о клиенте и средстве выполнения транзакции (например, карте) для дальнейшей ее передачи в UPOS-агент (200), размещенный на устройстве осуществления транзакций (300).

UPOS-агент (200) взаимодействует с POS-терминалом (100) с помощью интерфейсного модуля (203). Подключение терминала (100) к UPOS-агенту (200) может осуществляться с помощью локальной сети, например USB, RS-232, ЛВС, или посредством беспроводной сети посредством протоколов передачи данных Bluetooth или ZigBee. Соединение по ЛВС может реализовываться посредством использования транспортного протокола передачи данных TCP/IP или UPD. Также соединение может осуществляться за счет беспроводной сети с помощью таких средств, как GPRS-модем, GSM-модем, 4G-модем, Wi-Fi-адаптер, Ethernet-адаптер.

Основной функцией UPOS-агента (200) является маршрутизация данных и команд сервера (400), POS-терминалов (100) и устройства осуществления транзакций (300). UPOS-агент (200) обеспечивает управление операциями в активном режиме.

В частном варианте UPOS-агент (200) может являться программной или аппаратной частью непосредственно POS-терминала (100).

С помощью модуля маршрутизации (201) обеспечивается маршрутизация данных сервера (400) между UPOS-агентом (200) и POS-терминалом (100). Связь с сервером (400) осуществляется через соответствующий интерфейсный модуль (202) для взаимодействия по получению команд со стороны сервера (400) и передачи ответа сервера (400) в устройство (300).

Модуль интерфейса кассира (204) обеспечивает отображение на дисплее устройства (300) интерфейса для обработки транзакций, осуществляемых с помощью POS-терминала (100).

Обработка команд для осуществления операций с POS-терминалами (100) выполняется с помощью процессора (250) устройства выполнения транзакций (300) с последующей их передачей через сетевое устройство (260) на сервер (400). Сетевое устройство (260) должно обеспечивать соединение посредством сети Интернет между устройством (300) и сервером (400).

На фиг. 3 представлена схема UPOS-сервера (400). Модуль (401) настройки параметров POS-терминала предназначен для проверки текущего состояния POS-терминалов (100), подключенных к соответствующему агенту (200). Модуль (401) обеспечивает диагностику технического состояния POS-терминалов (100) и обновление их ПО для исключения ошибок в части обработки транзакционных сообщений.

UPOS-сервер (400) устанавливает соединение с одним или более POS-терминалом (100) и проводит их опрос, запрашивая общие хеш-значения локального набора файлов, содержащихся на POS-терминалах (100).

Сервер (400) содержит подключенную базу данных (450), которая хранит эталонные хеш-значения параметров POS-терминалов (100). Получая информацию от POS-терминалов (100), сервер (400) выполняет проверку полученных значений с терминалов с эталонными значениями. При несовпадении значений UPOS-сервер (400) передает на терминал (100) список файлов и ожидаемое хеш-значение каждого из них. POS-терминал (100) в ответ осуществляет проверку полученного списка и сличает требуемые хеш-значения со своими локальными файлами. Файлы с несовпадающим хеш-значением или отсутствующие на POS-терминале (100) сразу же загружаются с UPOS-сервера (400) по протоколу HTTP.

Модуль (402) правил обслуживания карт обеспечивает формирование правил выполнения транзакций, а также принятие решений по выполнению транзакции. Если во время этого процесса появляются какие-либо подозрения насчет мошенничества, то в осуществлении транзакции отказывается.

Также многое зависит и от типа банковской карты. К примеру, обслуживание дебетовых и кредитных карт имеет определенные различия. Также имеет значение и установленный банком приоритет авто-

ризации. Если карточка успешно проходит все проверки, то эмитент может одобрить операцию в рамках транзакции, а сам ответ поступает прямиком на POS-терминал (100). Например, перевод средств с карты на карту, осуществление покупки товара, возврат средств на карту, отмена транзакции и т.п. Модуль (402) также учитывает тип карты и процесс взаимодействия с ними.

Модуль (403) финансовых отчислений обеспечивает формирование правил изменения суммы транзакционной операции на основании информации о карте клиента (скидки, комиссии, штрафы, бонусы и т.п.). Также с помощью данного модуля осуществляется формирование дополнительных отчислений, не связанных с основной транзакцией, в частности чаевые, пожертвования в благотворительные фонды, возврат части суммы на счет клиента (кешбэк) и т.п.

Модуль формирования чеков (404) осуществляет генерирование данных, передаваемых на печать чековым принтером POS-терминала (100).

Модуль формирования реквизитов (405) осуществляет формирование платежной информации для ее передачи в банк.

Модуль (406) обеспечивает сетевое взаимодействие посредством сети Интернет с сервером авторизации транзакций (500). Модуль (406) может выполняться в виде Ethernet-адаптера, GSM-модуля (GPRS, LTE, 5G), Wi-Fi модуля, модуля спутниковой связи и т.п.

База данных (450) сервера также содержит базу терминалов и соответствующих параметров, которая используется для обновления ПО POS-терминалов (100).

Важной частью заявленной системы является также обеспечение защиты данных от несанкционированного доступа к транзакционной информации или данных по карте клиента. Для этого применяются следующие методы аутентификации и авторизации.

POS-терминал (100) дополнительно комплектуется ПИН-падом (109) со встроенным криптомодулем, обеспечивающим безопасное хранение KLK-ключа, а также ПИН-ключа и MAC-ключа. KLK-ключ является транспортным ключом для удаленной загрузки криптографических ключей (мастер-ключей). Длина каждого из ключей может быть как одинарной (DES), так и тройной (Triple DES).

Генерация ПИН-блока (ANSI X.9.8) выполняется с применением ПИН-ключа. Шифрование данных трафика осуществляется с применением MAC-кода (ANSI X.9.19) и TripleDES шифрования. В некоторых вариантах осуществления технического решения для шифрования ПИН-ключа может использоваться одна из следующих схем управления ключами: Derived Unique Key Per Transaction (ANSI X9.24), Fixed Key, Master Key/Session Key. Передача ПИН-блока осуществляется с использованием ключей шифрования RSA с длиной модуля ключа не менее 1024 битов.

Как представлено на фиг. 4, ключ KLK используется для генерации ПИН-ключа и MAC-ключа. POS-терминал (100) может хранить несколько пар ПИН/MAC-ключей в соответствии с количеством заданных "отделов". Для каждого "отдела" создается своя пара ПИН/MAC-ключей. Все ключи и их компоненты генерируются по случайному (псевдослучайному) закону. Алгоритм генерации случайных чисел проходит статистические тесты в соответствии с FIPS 140-2 (Level 3). За счет этого компрометация сгенерированного ключа становится возможной только при сговоре как минимум двух авторизованных лиц.

Для защиты целостности сообщений, передаваемых между POS-терминалом (100) и сервером (400), используется MAC-кодирование. Для формирования/проверки MAC-кода, необходимо выполнить на блоке данных передаваемых параметров процедуру ANSI X9.19.

Для MAC-ключа одинарной длины (8 байт) процедура имеет вид, представленный на фиг. 5. Для MAC-ключа двойной длины (16 байт) процедура имеет вид, представленный на фиг. 6.

Существует четыре основных режима использования MAC-кодирования:

1) не использовать;

2) использовать только для основных операций;

3) использовать для всех операций (за исключением смены ключей);

4) использовать шифрованные форматы.

В случае, если сервер (400) при проверке MAC-кода запроса обнаруживает несовпадение, он формирует POS-терминалу (100) ответ с кодом 98 и сообщением "М.КОД НЕВЕРЕН" (если это основная операция), либо '9' (если это сверка итогов), либо 'RB...599' (если это выгрузка пакета). POS-терминал проверяет MAC-код в ответе сервера (400) и в случае его совпадения обрабатывает код ответа штатным образом. В противном случае POS-терминал отвечает серверу (400) символом nak, по которому сервер (400) повторяет передачу ответа. При повторном получении ответа с неверным MAC-кодом POS-терминал разрывает соединение, после чего проверяет код ответа. В случае получения кода 98 (либо 9 для сверки итогов, либо RB..599 для выгрузки пакета) POS-терминал выдает оператору полученное от сервера сообщение, после чего возвращается в исходное состояние, считая операцию невыполненной. В противном случае (MAC-код в ответе не совпал и код ответа не равен 98) POS-терминал действует так, как если бы ответ сервера вообще не был получен.

В настройках POS-терминала (100) предусматривается возможность установки любого из этих режимов, что реализуется за счет криптомодуля ПИН-пада (109).

При использовании каналов связи общего пользования, легко подверженных угрозе перехвата данных (GSM-модем, GPRS-модем, Интернет), между терминалом (100) и UPOS-сервером (400) применяют-

ся защищенные (шифрованные) форматы обмена данными, базирующиеся на форматах VISA-II.

Шифрование исходного блока VISA-II (V) выполняется следующим образом: POS-терминал (100) вычисляет последовательность S как первые 8 байт из хеш-значения блока V, вычисленного по алгоритму SHA-1: S=[SHA1(V)]0..7.

С помощью ПИН-пада (109) или иного криптомодуля, хранящего MAC-ключ M, терминал (100) вычисляет MAC-код K над последовательностью S: K=MACM(S)=DESM(S).

Полученное значение K используется как ключ для программного шифрования блока V в режиме CBC: B=DESK(V).

При расшифровке сообщения сервер (400) выполняет аналогичные действия. С помощью программного или аппаратного криптомодуля вычисляет значение: K=MACM(S)=DESM(S).

С помощью вычислительной обработки расшифровывает блок данных B: V=DESK-1(B).

При работе в шифрованном режиме MAC-код внутри блока VISA-II не используется. Для проверки правильности расшифровки запроса сервер (400) сверяет полученные параметры с номером POS-терминала (100) с данными, идентифицирующими номер POS-терминала (100) внутри расшифрованного блока, а также вычисляет хеш-значение по расшифрованному сообщению, V и сравнивает его первые 8 байт со значением S. Если обнаружено несовпадение, сервер (400) отвечает POS-терминалу (100) о необходимости повторной передачи запроса. Если после трехкратной передачи запроса сервер (400) не может корректно его расшифровать, то связь между сервером (400) и POS-терминалом (100) разрывается.

POS-терминал (100) осуществляет проверку ответа, полученного от сервера (400), следующим образом. Если в расшифрованном ответе поля внутри блока, характеризующие первую и вторую части номера терминала не совпадают с реквизитами POS-терминала (100), POS-терминал осуществляет дальнейшее функционирование в обычном режиме без каких-либо действий.

При использовании шифрованных форматов совместно с динамической схемой ключей запрос и ответ на смену ключей всегда передаются в нешифрованном виде. Это единственный тип запроса, для которого не применяются ни MAC-код, ни шифрование. Запрос на сверку итогов с одновременной сменой ключей (транзакция 5F) подчиняется обычным правилам для сверки итогов (т.е. содержит MAC-код или шифруется). Описываемые форматы взаимодействия POS-терминала (100) с сервером (400) допускают две схемы использования ключей для MAC-кода и PIN-блока.

Первая схема - статическая, которая предполагает, что формирование MAC-кода и шифрование PIN-блока осуществляется непосредственно на мастер-ключах, неизменных в течение всего периода работы POS-терминала.

При второй (динамической) схеме POS-терминал (100) регулярно выполняет вспомогательный запрос "смена ключей" и получает в ответе от сервера (400) новые значения рабочих ключей для MAC-кода и PIN-блока, зашифрованные под соответствующими мастер-ключами. Полученные зашифрованные значения POS-терминал хранит за пределами криптомодуля и передает в него при выполнении операций с MAC-кодом или PIN-блоком. В терминологии международных платежных систем такая схема называется "master/sessionkey" и является одной из стандартных. В настройках POS-терминала (100) должен быть параметр, определяющий, по какой схеме POS-терминал работает с ключами - статической или динамической. Если включено использование динамической схемы, то алгоритм работы POS-терминала меняется следующим образом:

1. POS-терминал должен иметь внутренний флаг, указывающий, были ли получены сеансовые ключи или нет. Этот флаг должен сбрасываться при загрузке ПО или параметров в POS-терминал (100), а устанавливаться после первой успешной операции смены ключей (или сверки итогов с одновременной сменой ключей, транзакция 5F). Перед началом платежной операции POS-терминал должен проверять этот флаг и, если он не установлен, выдавать сообщение "Выполните сверку итогов".

2. Используемую длину ключей (одинарную или двойную) POS-терминал определяет автоматически на основании ответа на смену ключей.

3. При использовании динамической схемы при получении на любой запрос ответа "MAC-код неверен" POS-терминал (100) должен выполнить смену ключей (по возможности без разрыва связи) и повторить исходный запрос (также по возможности без разрыва связи). При повторном получении ответа "MAC-код неверен" POS-терминал должен действовать так, как если бы ответ на исходный запрос не был получен вообще.

4. При использовании динамической схемы совместно с шифрованными форматами возможна ситуация, когда из-за расхождения сеансовых ключей сервер (400) не может расшифровать запрос и определить его тип. В этом случае сервер (400) возвращает "пустой" ответ, состоящий из трех символов stxetxetx. Такой ответ POS-терминал (100) должен интерпретировать как ответ "MAC-код неверен" и действовать, как описано выше (инициировать смену ключей и повторный запрос).

5. При выполнении сверки итогов вместо транзакции 50 POS-терминал (100) должен использовать транзакцию 5F. В этом случае отдельный запрос "смена ключей" (транзакция 51) потребуется только в аварийный случаях (например, при обрыве связи в момент транзакции 5F).

6. ПИН-пад (109) POS-терминала позволяет удаленно загружать мастер-ключи, зашифрованные на некотором "супер-мастер-ключе" KLK.

7. Транзакция 51 (смена ключей) выполняется следующим образом:

POS-терминал (100) опрашивает ПИН-пад (109) и выясняет, какие ключи в него загружены, а какие нет. Если оказывается, что в ПИН-паде (109) нет KLK, или что оба мастер-ключа (ПИН- и MAC-) уже загружены, то POS-терминал (100) выполняет смену сеансовых ключей, указывая в поле "Тип ключа, подлежащего смене" символ 'A';

если же ПИН-пад (109) сообщает, что в нем есть KLK, но нет ПИН- или MAC-мастер-ключа, то POS-терминал (100) выполняет смену мастер-ключей, указывая в поле "Тип ключа, подлежащего смене" символ 'F';

независимо от того, какую смену пытался выполнить POS-терминал (100) (сеансовых или мастер-ключей), он должен быть готов к тому, что в ответе ему придет ноль, два или четыре ключа, т.е. по инициативе сервера (400) возможна смена мастер-ключей в ответ на запрос смены сеансовых ключей;

если в ответе нет ключей, POS-терминал (100) оставляет текущие сеансовые и мастер-ключи неизменными, если при этом код ответа не равен '0', POS-терминал (100) выдает сообщение "Ошибка смены ключей" и прекращает выполнение текущей операции;

если POS-терминал (100) получил два ключа, то это сеансовые ключи. POS-терминал (100) должен сохранить их в своих настройках. Мастер-ключи, хранимые в ПИН-паде (109), при этом не меняются;

если POS-терминал (100) получил четыре ключа, то первые два являются сеансовыми ключами (POS-терминал сохраняет их в своих настройках и далее использует как обычно), а вторые два - мастер-ключами (POS-терминал должен прогрузить их в ПИН-пад).

8. Сеансовый ключ имеет такую же длину, что и мастер-ключ (одинарную или двойную). Если длина ключа двойная, то сеансовый ключ шифруется мастер-ключом.

Далее рассмотрим на примере начало взаимодействия POS-терминала (100) и UPOS-сервера (400).

Сервер (400) при инсталляции генерирует ключевую пару RSA с длиной модуля 2048 бит. Публичный ключ сервера Spub включается в дистрибутивный комплект ПО POS-терминала (100) вместе с данными IP-адреса и номера порта сервера (400).

ПО POS-терминала (100) при первом запуске генерирует собственную ключевую пару RSA с заданной длиной модуля, меньшей чем Spub, например 1536 бит. Сгенерированная пара ключей сохраняется в памяти POS-терминала (100) в локальных файлах, недоступных для внешнего считывания.

Шифрование данных между POS-терминалом (100) и сервером (400) выполняется на ключе K длиной 24 байта по алгоритму TripleDES с тройной длиной ключа. Текущее значение ключа K также хранится в локальном файле POS-терминала (100), недоступном для внешнего считывания. На стороне сервера (400) значение ключа K хранится в защищенном хранилище БД (450).

После генерации ключевой пары выполняется активация POS-терминала. В ходе процедуры активации в POS-терминал вводится значение TerminalID и код активации (KA) - уникальный пароль для данного TerminalID.

Введенные значения TerminalID и KA POS-терминал (100) объединяет в буфер. Туда же POS-терминал (100) добавляет свой публичный ключ Tpub, серийный номер SN и контрольное значение текущего ключа K (KCVK). Поскольку как таковой ключ K в POS-терминале отсутствует, то значение KCVK=000000.

Осуществляется формирование WK (Working Key)=TerminalID | | SN | | KA | | Tpub | | KCVK. Итоговая длина WK не должна превышать длину модуля ключа Spub. Поэтому необходимо, чтобы длина модуля Tpub была меньше длины модуля Spub как минимум на 27 байт.

Далее POS-терминал (100) шифрует блок A публичным ключом сервера и получает блок B: B=RSASpub(A).

POS-терминал (100) устанавливает связь с сервером (400) и отправляет ему блок B. Сервер (400) расшифровывает блок B своим секретным ключом, по значению TerminalID сервер (400) обнаруживает нужную запись в БД (450) и сверяет присланное значение SN с хранящимся в базе. Если значения не совпадают (а при первичной активации так будет обязательно), то сервер (400) проверяет значение KA. Если оно правильное, то новое значение SN сохраняется в базе (450) и проверка серийного номера признается успешной.

Далее сервер (400) сверяет значение KCVK с хранящимся в БД (450). Если оно не совпадает (а при первичной активации так будет обязательно), сервер (400) генерирует новый случайный ключ K, сохраняет его в БД (450), шифрует его ключом Tpub и возвращает POS-терминалу (100).

POS-терминал (100) расшифровывает ключ K и сохраняет его в своем локальном файле. Теперь POS-терминал (100) может принимать от сервера (400) команды, зашифрованные ключом K.

В дальнейшем выполнение каждой операции на POS-терминале (100) будет начинаться с такого же обмена. Только вместо значения KA POS-терминал (100) будет подставлять 0. Поскольку TerminalID и SN не менялись с момента первоначальной активации, сервер (400) будет считать проверку SN успешной, не обращая внимания на заведомо неверное значение KA. Значение KCVK также будет совпадать, но сервер (400) имеет право в любой момент сгенерировать и отправить POS-терминалу (100) новое значение ключа K, если этого будет требовать процедура обработки параметров транзакции.

Далее рассмотрим пример выполнения транзакции (600) с помощью заявленной системы со ссыл-

ками на фиг. 7 и 8.

На устройстве выполнения транзакции (300) оператор инициирует процесс оплаты, и соответствующие данные с помощью модуля UPOS-агента (200) передаются для инициации распознавания средства осуществления оплаты на POS-терминале (100) под управлением UPOS (этап 601). На дисплее POS-терминала (100) отображается сумма транзакции, и оператор устройства (300) осуществляет ее ввод в терминал (этап 602). Далее POS-терминал (100) генерирует запрос на выполнение транзакции, который содержит тип операции и сумму (этап 603). Запрос передается через модуль UPOS-агента (200) на UPOS-сервер (400).

На следующем этапе (604) на основании полученного запроса от POS-терминала (100) сервер (400) формирует команду на обработку данных транзакции и направляет ее на POS-терминал (100). В ответ на полученную команду сервера (400) POS-терминал (100) инициирует процесс верификации платежного средства (карты) клиента и генерирует соответствующее сообщение, выводимое на дисплее POS-терминала (100). После чего выполняется распознавание карты пользователя (605), в частности обработка номера PAN (Primary Account Number) карты. После получения данных карты на POS-терминале (100) информация шифруется и передается по защищенному каналу передачи данных (например, SSL защищенного канала) на сервер (400).

В ответ на полученные данные по карте клиента, полученные от POS-терминала (100), сервер (400) анализирует БИН карты (банковский идентификационный номер) (этап 606). По итогам проверки БИН номера карты сервер (400) формирует команду на генерирование криптограммы ARQC (Authorisation Request Cryptogram) (607) и передает ее на POS-терминал (100). POS-терминал (100) с помощью модуля шифрования (105) инициирует формирование криптограммы. В процессе формирования криптограммы POS-терминал (100) определяет процесс зерификации для типа карты клиента, для чего выполняется анализ CVM карты (этап 608).

В основе формирования и проверки криптограмм лежит алгоритм 3DES. Эмитент и карта владеют общим секретным ключом MKac (Application Cryptogram Master Key). В начале транзакции карта генерирует на основе MKac сессионный ключ SKac (Application Cryptogram Session Key). Криптограмма ARQC длиной, например, 8 байт генерируется картой с помощью алгоритма MAC на сессионном ключе SKac с использованием данных транзакции.

В процессе транзакции сгенерированная картой криптограмма ARQC отправляется серверу (400), который сверят пришедшую ARQC с криптограммой, которую рассчитал самостоятельно. Для этой операции сервером (400) генерируется сессионный ключ, затем на основании пришедших данных транзакции рассчитывается собственный ARQC. Если собственный (сгенерированный эмитентом) ARQC и ARQC карты сходятся - карта подлинная.

Вот пример классического CVM: 4403410342031E031F02.

Расшифровка выглядит следующим образом:

1	4403	Enciphered PIN - if terminal supports the CVM
2	4103	Offline Plain text PIN - if terminal supports the CVM
3	4203	Online PIN - if terminal supports the CVM
4	1E03	Signature - if terminal supports the CVM
5	1F02	No CVM - If not unattended cash and not manual cash and not purchase

При выполнении анализа CVM определяется, установлен ли на карте клиента запрос на ввод PIN-кода. Если ввод кода необходим, то осуществляется его ввод (610) в POS-терминал (100). В ответ на получение на этапе (610) PIN-кода выполняется проверка его правильности. Если PIN-код введен корректно (612) или запрос ввода PIN на карте не установлен, то осуществляется формирование криптограммы (609) с помощью модуля шифрования (105) POS-терминала (100).

В уровне техники различают два способа верификации PIN-кода: онлайн PIN, когда значение PIN-кода проверяется эмитентом карты или авторизованным эмитентом сервером, и оффлайн PIN, когда значение PIN-кода проверяется микропроцессорной картой. Значение PIN-кода передается для проверки серверу или карте в виде PIN-блока размером 8 байтов. В соответствии с ISO 9654-1 с этой целью должны использоваться форматы ISO-0, ISO-1, ISO-2, ISO-3.

На этапе (611) проверяют, введен ли PIN-код онлайн или оффлайн. Если PIN-код введен офлайн, осуществляет проверку кода на микропроцессорной карте, иначе генерируют криптограмму для отправки на сервер (400).

Микропроцессорная карта называется Chip&PIN-картой, если способ проверки ПИН-кода офлайн PIN (независимо от способа передачи ПИН-кода - в защищенном или незащищенном виде) является самым приоритетным в списке CVM List в условиях выполнения данной операции. POS-терминал поддерживает способ офлайн PIN, если он поддерживает защищенную и открытую передачу ПИН-кода на карту. Тогда перенос ответственности Chip&PIN Liability Shift формулируется следующим образом: если

Chip&PIN-карта используется в POS-терминале, не поддерживающем офлайн PIN, то вся ответственность за потерянные/похищенные (Lost/Stolen) карты, а также неполученные карты (NRI) переносится на банк-эквайер.

В результате рекомендуемая платежными системами приоритетность правил верификации держателя карты в CVM List при выполнении операции с использованием DDA/CDA-карты в POS-терминале имеет следующий вид:

1. Enciphered Offline PIN.

2. Plaintext Offline PIN; 3. Online PIN.

4. Signature.

5. No CVM.

В ходе проверки PIN также проверяется количество попыток ввода кода (613). И если количество попыток исчерпано при неправильном вводе PIN-кода, то POS-терминал формирует параметр, указывающий на то, что клиент не верифицирован (614).

Сформированная криптограмма передается на сервер (400) для генерирования авторотационного запроса (615), который передается от UPOS-сервера (400) на сервер авторизации транзакций (500) (процессинговый сервер) (этап 616).

Сервер авторизации транзакций (500) осуществляет обработку запроса (617), в ходе которой на основании полученных данных сервер (500) одобряет выполнение транзакции или отказывает в ее выполнении.

При положительной обработке данных транзакции сервер авторизации (500) формирует сообщение на UPOS-сервер (400). На основании полученного сообщения от сервера авторизации (500) UPOS-сервер (400) генерирует команду на создание второй криптограммы (618) с информацией, подтверждающей выполнение транзакции, которая передается на POS-терминал (100).

В ответ на полученную команду от сервера (400) POS-терминал (100) осуществляет формирование второй криптограммы (619).

Сформированная криптограмма передается на UPOS-сервер (400) через UPOS-агент (200). Полученная криптограмма анализируется сервером (400) (этап 620). Сервер (400) по похожему алгоритму формирования криптограммы на основе динамических данных транзакции и данных ответа генерирует ARPC (Authorisation Response Cryptogram) и отсылает эту криптограмму назад карте. В тот момент, когда карта подтвердит пришедший ARPC, взаимная аутентификация карты и эмитента выполнена.

При положительной проверке криптограммы сервер (400) генерирует команду на подготовку чека (621), которая передается на POS-терминал (100). В ответ на полученную команду сервера (400) POS-терминал (100) отображает статус выполнения транзакции и посредством принтера осуществляет печать чека. В случае если проверка криптограммы не была осуществлена, то сервер (400) генерирует запрос для отмены выполнения транзакции (623), которая передается на сервер авторизации (500). Сервер (500) выполняет обработку полученного запроса (624) и генерирует ответное сообщение для UPOS-сервера (400).

UPOS-сервер (400) в ответ на сообщение авторизации отмены операции выполняет формирование команды (625) для POS-терминала для отмены транзакции. Упомянутая команда направляется на терминал (100), в ответ на которую клиенту выводится сообщение об отказе обработки карты (626).

На фиг. 9 представлена общая схема вычислительного устройства (700), которое может выполнять функции устройства выполнения транзакций, UPOS-сервера и сервера авторизации транзакций.

Вычислительное устройство (700) в общем случае содержит такие компоненты, как один или более процессоров (701), по меньшей мере одну память (702), средство хранения данных (703), интерфейсы ввода/вывода (704), средство ввода/вывода (705), средство сетевого взаимодействия (706).

Процессор (701) устройства выполняет основные вычислительные операции, необходимые для функционирования модулей исполняющего команды устройства. Процессор (701) исполняет необходимые машиночитаемые команды, содержащиеся в оперативной памяти (702).

Память (702), как правило, выполнена в виде ОЗУ и содержит необходимую программную логику, обеспечивающую требуемый функционал.

Средство хранения данных (703) может выполняться в виде HDD, SSD-дисков, рейд массива, флэш-памяти, оптических накопителей информации (CD, DVD, MD, Blue-Ray-дисков) и т.п. Средства (703) позволяют выполнять долгосрочное хранение различного вида информации.

Интерфейсы (704) представляют собой стандартные средства для подключения и работы нескольких устройств, например USB, RS232, RJ45, LPT, COM, HDMI, PS/2, Lightning, FireWire и т.п.

Выбор интерфейсов (704) зависит от конкретного исполнения устройства (700), которое может представлять собой персональный компьютер, мейнфрейм, серверный кластер, тонкий клиент, смартфон, кассовый аппарат и т.п.

В качестве средств ввода/вывода данных (705) могут использоваться: клавиатура, джойстик, дисплей (сенсорный дисплей), проектор, тачпад, манипулятор мышь, трекбол, световое перо, динамики, микрофон и т.п.

Средства сетевого взаимодействия (706) выбираются из устройств, обеспечивающих сетевой прием

и передачу данных, например Ethernet карту, WLAN/Wi-Fi модуль, Bluetooth модуль, BLE модуль, NFC модуль, IrDa, RFID модуль, GSM модем и т.п. С помощью средств (705) обеспечивается организация обмена данными по проводному и/или беспроводному каналу передачи данных, например WAN, PAN, ЛВС (LAN), Интранет, Интернет, WLAN, WMAN или GSM.

В настоящих материалах заявки было представлено предпочтительное раскрытие осуществления заявленного технического решения, которое не должно использоваться как ограничивающее иные, частные воплощения его реализации, которые не выходят за рамки испрашиваемого объема правовой охраны и являются очевидными для специалистов в соответствующей области техники.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система управления POS-терминальной сети, содержащая по меньшей мере один UPOS-сервер, связанный с сервером авторизации транзакций, а также объединенный каналом передачи данных с устройством осуществления финансовых транзакций, содержащим модуль UPOS-агента, к которому подключен один или более POS-терминалов, осуществляющих функционирование посредством ПО UPOS, в которой

модуль UPOS-агента выполнен с возможностью обеспечении маршрутизации данных между UPOS-сервером, POS-терминалами и устройством осуществления транзакций;

POS-терминал выполнен с возможностью приема клиентских запросов на выполнение транзакций, верификации клиентов, шифрования транзакционных данных клиентских запросов;

UPOS-сервер выполнен с возможностью мониторинга и контроля параметров POS-терминалов, управления работой POS-терминала, генерирования сценариев обработки транзакций и обмена данными с сервером авторизации транзакций, обновления параметров программного обеспечения POS-терминала, причем

UPOS-сервер выполнен с возможностью запрашивать и получать общие хеш-значения локального набора файлов, содержащихся на POS-терминалах, сравнивать полученные с POS-терминалов значения с эталонными значениями, хранящимися в подключенной к UPOS-серверу базе данных эталонных хеш-значений параметров POS-терминалов, в случае несовпадения значений передавать на POS-терминал список файлов и ожидаемое хеш-значение и после проверки POS-терминалом требуемых хеш-значений со своими локальными файлами загружать на POS-терминал файлы с несовпадающим хеш-значением или отсутствующие файлы.

2. Система по п.1, характеризующаяся тем, что модуль UPOS-агента реализует генерирование интерфейса обработки транзакций с помощью устройства осуществления финансовых транзакций.

3. Система по п.1, характеризующаяся тем, что UPOS-агент и связанные с ним POS-терминалы связаны посредством локального сетевого соединения или посредством вычислительной сети.

4. Система по п.3, характеризующаяся тем, что локальное соединение выбирается из групп RS-232, USB, ЛВС или их сочетания.

5. Система по п.3, характеризующаяся тем, что ЛВС обеспечивает соединение посредством TCP/IP протокола.

6. Система по п.5, характеризующаяся тем, что соединение осуществляется за счет устройства сетевой передачи данных POS-терминала, которое выбирается из группы: GPRS-модем, GSM-модем, 4G-модем, Wi-Fi адаптер, Ethernet-адаптер.

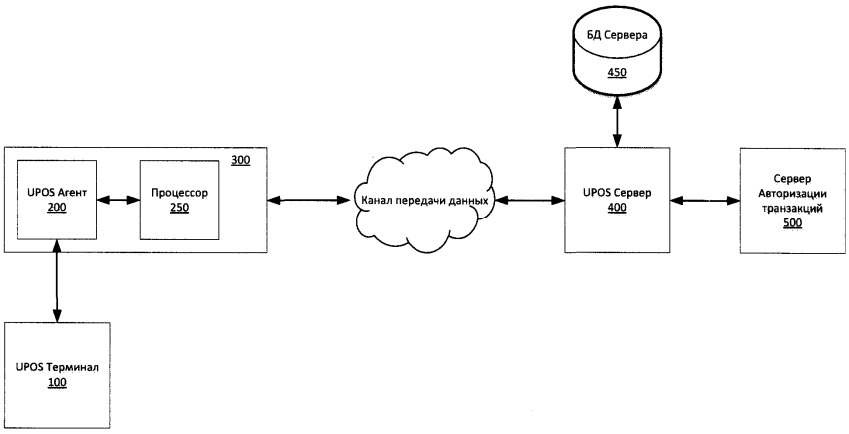
7. Система по п.1, характеризующаяся тем, что UPOS-сервер содержит модуль настройки параметров POS-терминалов.

8. Система по п.1, характеризующаяся тем, что UPOS-сервер содержит модуль обработки правил взаимодействия с банковскими картами.

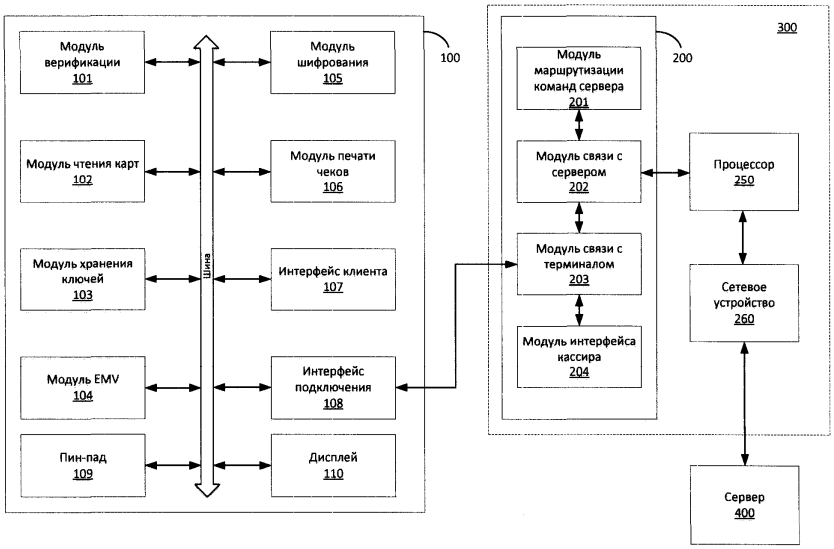
9. Система по п.1, характеризующаяся тем, что UPOS-сервер содержит модуль формирования финансовых отчислений, выполненный с возможностью генерирования в ответ на обработку транзакций посредством POS-терминалов дополнительных финансовых движений по счету клиента.

10. Система по п.9, характеризующаяся тем, что дополнительные финансовые движения выбираются из группы: скидки, учет бонусных средств на счете клиента, возврат части затраченной суммы оплаты или их сочетания.

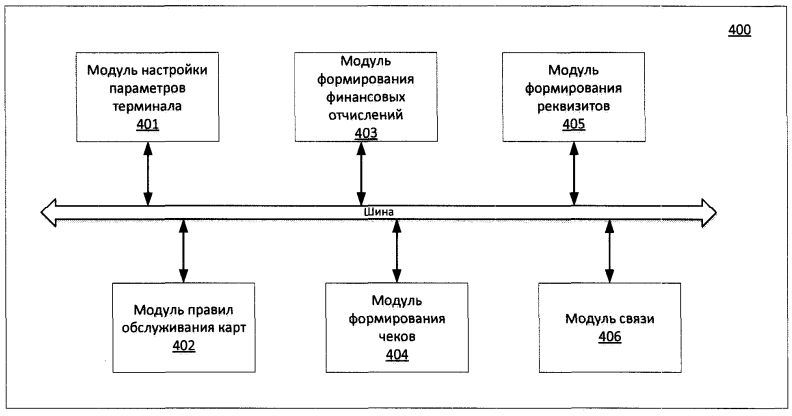
11. Система по п.1, характеризующаяся тем, что UPOS-сервер содержит модуль генерирования чеков.



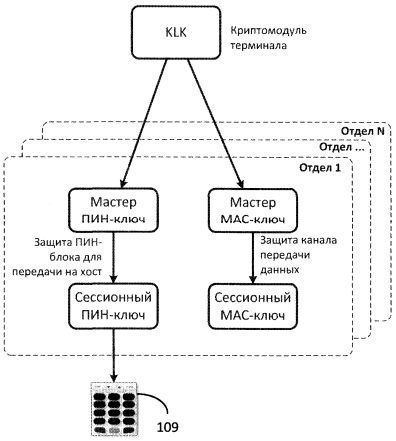
Фиг. 1



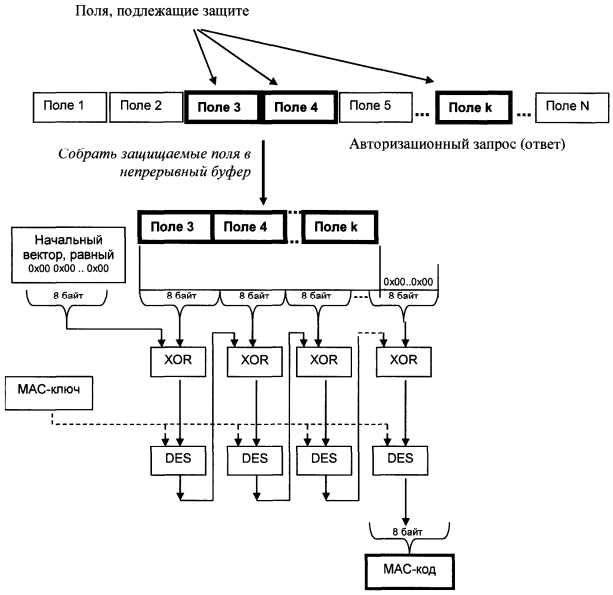
Фиг. 2



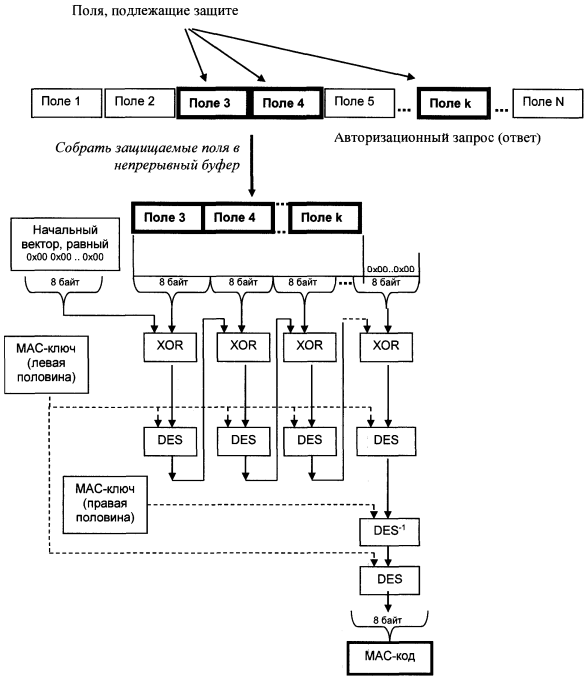
Фиг. 3



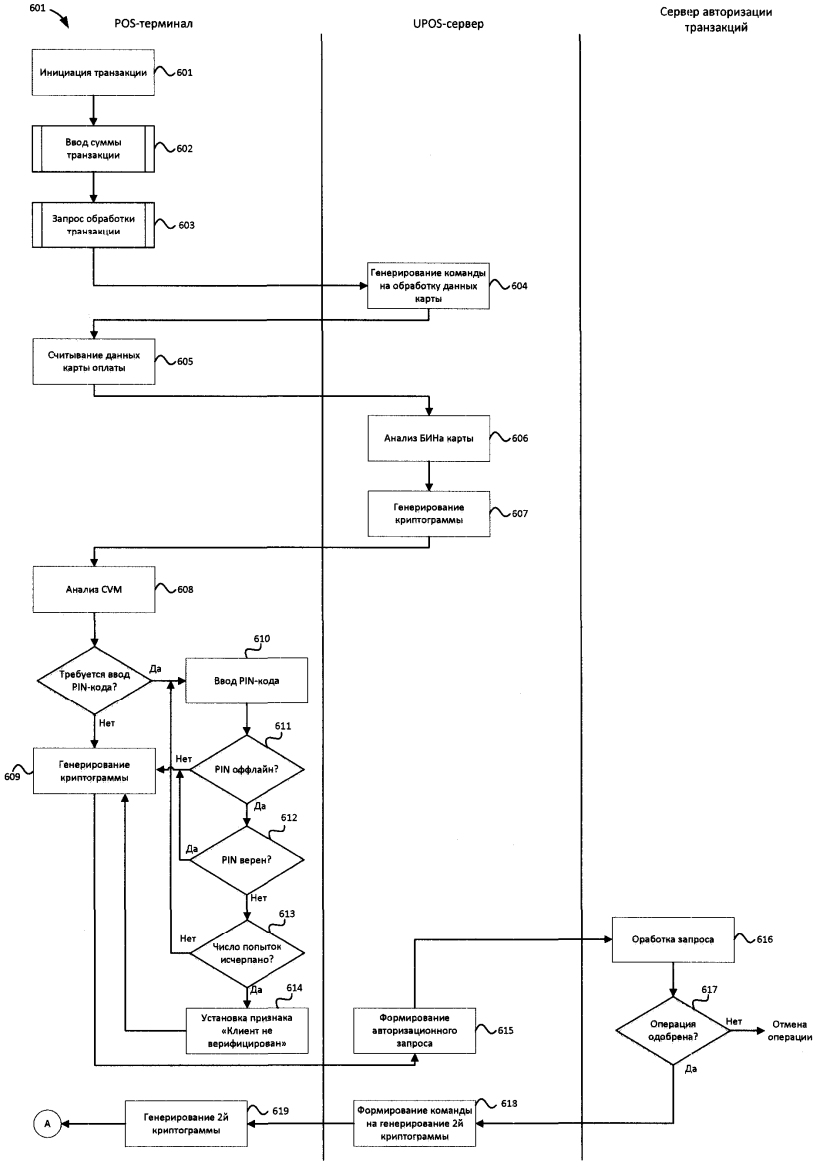
Фиг. 4



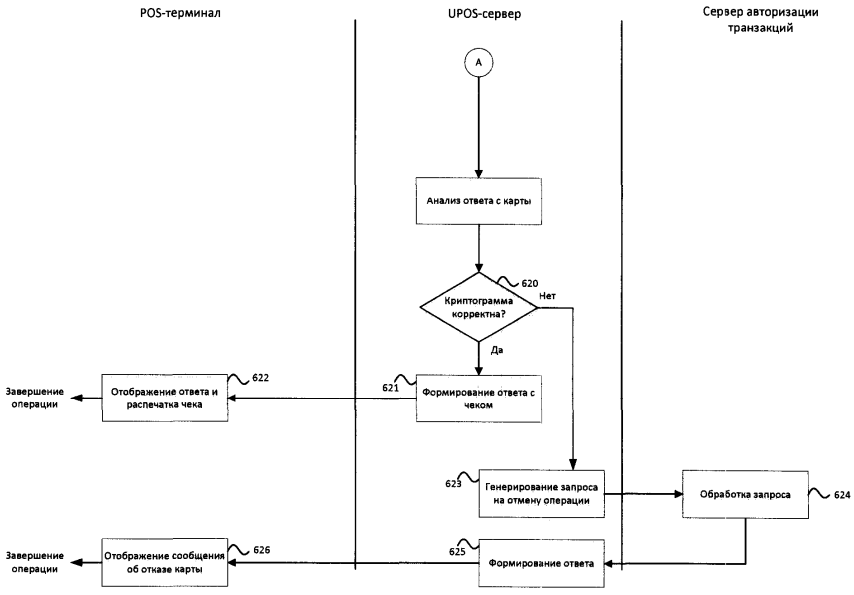
Фиг. 5



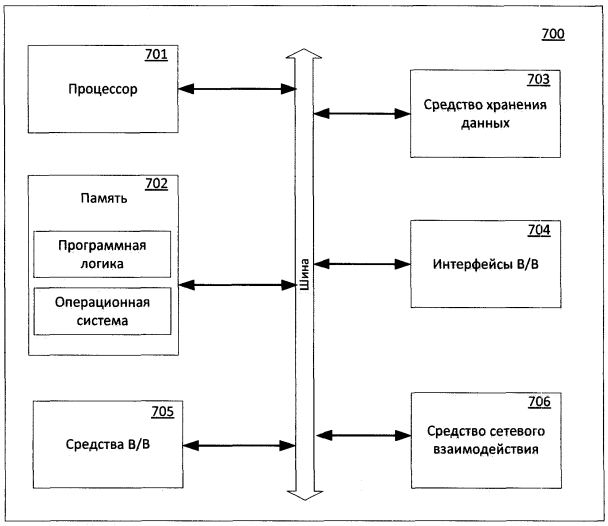
Фиг. 6


601
POS-терминал
UPOS-сервер
Сервер авторизации транзакций
Инициация транзакции
601
Ввод суммы транзакции
602
Запрос обработки транзакции
603
Генерирование команды на обработку данных карты
604
Считывание данных карты оплаты
605
Анализ БИНа карты
606
Генерирование криптограммы
607
Анализ CVM
608
610
Требуется ввод PIN-кода?
Да
Ввод PIN-кода
Нет
611
609
Генерирование криптограммы
Нет
PIN оффлайн?
Да
612
Да
PIN верен?
Нет
613
Нет
Число попыток исчерпано?
Да
614
Установка признака «Клиент не верифицирован»
Формирование авторизационного запроса
615
Оработка запроса
616
617
Операция одобрена?
Нет
Отмена операции
Да
A
Генерирование 2й криптограммы
619
Формирование команды на генерирование 2й криптограммы
618

Фиг. 7


POS-терминал
UPOS-сервер
Сервер авторизации транзакций
A
Анализ ответа с карты
620
Криптограмма корректна?
Нет
Да
Завершение операции
Отображение ответа и распечатка чека
622
621
Формирование ответа с чеком
623
Генерирование запроса на отмену операции
Обработка запроса
624
Завершение операции
Отображение сообщения об отказе карты
626
625
Формирование ответа

Фиг. 8


700
701
Процессор
703
Средство хранения данных
702
Память
Программная логика
Операционная система
Шина
704
Интерфейсы В/В
705
Средства В/В
706
Средство сетевого взаимодействия

Фиг. 9