РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 438 172** (13) **C2**

(51) МПК
G06F 21/20 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2008137231/08, 02.03.2007**

(24) Дата начала отсчета срока действия патента:
02.03.2007

Приоритет(ы):
(30) Конвенционный приоритет:
02.03.2006 US 60/778,282

(43) Дата публикации заявки: **27.03.2010** Бюл. № 9

(45) Опубликовано: **27.12.2011** Бюл. № **36**

(56) Список документов, цитированных в отчете о поиске: **US 2002/0120587 A1, 29.08.2002. US 6,836,765 B1, 28.12.2004. US 5,280,527 A, 18.01.1994. US 2005/0289052 A1, 29.12.2005. RU 50325 U1, 27.12.2005.**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **18.09.2008**

(86) Заявка PCT:
US 2007/063239 (02.03.2007)

(87) Публикация заявки PCT:
WO 2007/103831 (13.09.2007)

Адрес для переписки:
119296, Москва, а/я 113, пат.пов. Э.П.Песикову, рег.№ 204

(72) Автор(ы):
ДОМИНГЕС Бенедикто Х. (US),
ФИШЕР Даглас (US),
ЛИ Тимоти Му-чу (SG)

(73) Патентообладатель(и):
ВИЗА ИНТЕРНЕШНЛ СЕРВИС АССОШИЭЙШН (US)

(54) СПОСОБ И СИСТЕМА ДЛЯ ОСУЩЕСТВЛЕНИЯ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПРИ ТРАНЗАКЦИЯХ, СВЯЗАННЫХ С ЗАКАЗАМИ ПО ПОЧТЕ И ТЕЛЕФОНУ

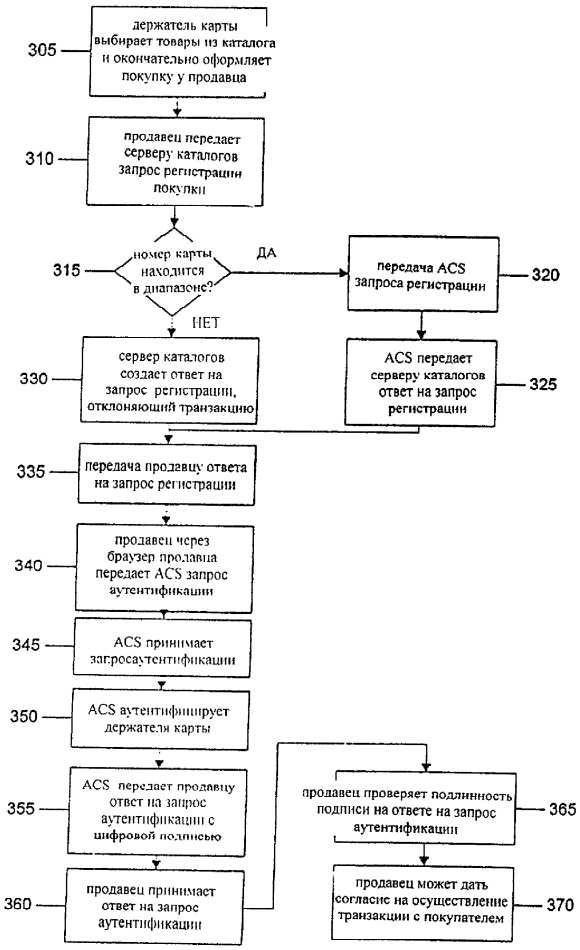
(57) Реферат:

Изобретение относится к средствам аутентификации транзакции. Техническим результатом является повышение защиты при аутентификации транзакций. В способе продавец вводит в систему продавца заказ по почте или телефону (MOTO), данные карты транзакции: номер карты, аутентификационную информацию, данные заказа, данные карты принимают по электронной почте или по телефону, системой продавца передают серверу запрос проверки регистрации, номер карты транзакции, индикатор, что информация держателя карты не будет им передана при запросе проверки регистрации, системой продавца принимают от сервера ответ на запрос, где указано, доступна ли аутентификация карты по ее номеру, если доступна - системой продавца принимают от сервера предложение аутентификации, без запроса конфиденциальной информации держателя карты, системой продавца вводят аутентификационную информацию держателя в предложение аутентификации, с помощью

RU 2438172 C2

RU 2438172 C2

системы продавца передают серверу запрос аутентификации, содержащий аутентификационную информацию, принимают от сервера аутентификации ответ на запрос аутентификации, в котором указано аутентифицирован ли держатель карты. 3 н. и 23 з.п. ф-лы, 4 ил.



Фиг. 3

RU 2438172 C2

RU 2438172 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 438 172** (13) **C2**

(51) Int. Cl.
G06F 21/20 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2008137231/08, 02.03.2007**

(24) Effective date for property rights:
02.03.2007

Priority:
(30) Priority:
02.03.2006 US 60/778,282

(43) Application published: **27.03.2010** Bull. 9

(45) Date of publication: **27.12.2011 Bull. 36**

(85) Commencement of national phase: **18.09.2008**

(86) PCT application:
US 2007/063239 (02.03.2007)

(87) PCT publication:
WO 2007/103831 (13.09.2007)

Mail address:
119296, Moskva, a/ja 113, pat.pov. Eh.P.Pesikovu, reg.№ 204

(72) Inventor(s):
DOMINGES Benedikto Kh. (US),
FIShER Daglas (US),
LI Timoti Mu-chu (SG)

(73) Proprietor(s):
VIZA INTERNEShNL SERVIS ASSOShIEhJShN (US)

RU 2438172 C2

(54) METHOD AND SYSTEM FOR PERFORMING TWO-FACTOR AUTHENTICATION IN MAIL ORDER AND TELEPHONE ORDER TRANSACTIONS

(57) Abstract:

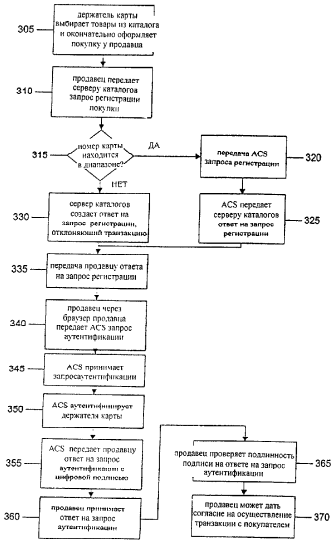
FIELD: information technology.

SUBSTANCE: in the method, a merchant enters the following transaction card data into the mail order or telephone order (MOTO) merchant system: card number, authentication information, order data; card data are received through electronic mail or over the telephone; the merchant system sends to the server a request to verify registration, transaction card number, an indicator that cardholder information will not be sent to them upon request for registration verification; the merchant system receives from the server a response to the request, where it is indicated whether card number authentication is accessible; if so, the merchant system receives from the server an authentication offer without request for confidential information of the cardholder; the merchant system enters the authentication information of the holder into the authentication offer; using the system, the merchant sends the server an authentication request containing authentication information; an authentication response is received from the server in which it is indicated whether the cardholder is authenticated.

EFFECT: high security during transaction authentication.

26 cl, 4 dwg

RU 2438172 C2



Фиг. 3

RU 2438172 C2

RU 2438172 C2

Ссылка на родственные заявки

Приоритет настоящей заявки основан на патентной заявке США №60/778282 "Method and System for Performing Two Factor Authentication in Mail Order and Telephone Order Transactions", поданной 2 марта 2006 г.

Предпосылки создания изобретения

При транзакции с использованием карты, такой как кредитная карта, кредитная карта, дебетовая карта, карта с хранимой суммой, банковская карта, карта постоянного покупателя, смарт-карта и/или т.п. важно удостовериться в том, что держатель карты является владельцем счета во избежание разнообразных проблем, таких как несанкционированное использование. Аутентификация держателя карты представляет собой процесс, в ходе которого проверяют право такого владения держателя карты. Например, при транзакции с предъявлением карты осуществляют аутентификацию держателя карты, когда представитель продавца проверяет, совпадает ли подпись на карте с подписью держателя карты на квитанции.

С развитием технологии организации и частные лица получили возможность участвовать в транзакциях, осуществляемых во множестве различных сред. Например, держатели карт могут участвовать в традиционных транзакциях с личным участием, транзакциях через Интернет, транзакциях по телефону и транзакциях через системы электронной почты. Во многих случаях держатели карт предпочитают осуществлять транзакции без необходимости личного посещения поставщика услуг. При этом держатель карты, возможно, хочет сэкономить время на езду и избежать связанных с этим затруднений, например, при покупках в розничной сети или при ожидании в очереди в банке, и осуществить эти транзакции, находясь у себя дома.

Растет объем транзакций без предъявления карты (CNP, от английского - Card not present), что по меньшей мере частично объясняется их удобством для держателей карт и увеличением объема продаж для продавцов. Тем не менее, по мере роста объема CNP-транзакций также увеличивается число мошеннических транзакций и денежных убытков из-за таких транзакций.

Предлагались различные решения с целью улучшения защиты операций электронной торговли и/или банковских операций в реальном времени, такие как двухфакторная аутентификация (например, компанией GPayment Pty. Ltd), одноразовые пароли (например, компанией Barclay PLC) и аутентификация по жетонам (например, компанией MasterCard International Inc.). Однако эти технические решения не реализованы применительно к транзакциям, связанным с заказами по почте и телефону (MOTO, от английского - mail order and telephone order) из-за уникальной сложности задач, которые ставят такие транзакции.

Например, в системе защиты могут возникать слабые места, когда в MOTO-транзакциях используют постоянные пароли. Постороннее третье лицо может получить постоянный пароль путем перехвата транзакции и воспроизведения переданных данных с целью расшифровки данных счета и пароля. Посторонним третьим лицом может являться, например, лицо, перехватывающее информацию, которой обменивается держатель карты и продавец или продавец и эмитент карты. В качестве альтернативы посторонним третьим лицом может являться продавец и/или его представитель.

Решения для улучшения защиты включают использование статических данных, таких как информация, хранящаяся в поле для контрольного кода карты (CVV2, от английского - Card Verification Value 2), информация службы проверки адреса, срок действия, предоставление полномочий контроль и т.п. Поле для CVV2 служит для

подтверждения того, что карта для осуществления транзакции принадлежит держателю карты. Когда держатель карты предоставляет продавцу CVV2, продавец включает CVV2 в направляемый эмитенту запрос авторизации, при ответе на который продавцу сообщают, является ли предоставленный CVV2 действующим.

Одним из недостатков таких процедур статической аутентификации является то, что коды аутентификации не меняются при каждой транзакции. Соответственно третье лицо, которое получило доступ к карте даже на короткое время, имеет возможность скопировать информацию и использовать ее втайне от держателя карты.

Другим недостатком процедур статической аутентификации является то, что в ходе таких процедур обычно осуществляют только проверку наличия карты для транзакции, а не аутентификацию держателя карты. Однако аутентификация держателя карты обеспечивает лучшую защиту, чем проверка карты для транзакции. Например, при аутентификации держателя карты, в отличие от аутентификации карты для транзакции, эмитенты карт получают достаточное неопровержимое доказательство, чтобы гарантировать продавцу защиту от убытков.

Также разрабатываются технологии динамической аутентификации с целью облегчения аутентификация держателя карты в среде МОТО-транзакций. Такие технологии включают аутентификацию по голосу, звуковую аутентификацию (т.е. карты, генерирующие изменяемые звуки) и одноразовые пароли. Одним из недостатков таких технологий динамической аутентификации является то, что они лишь частично решают задачу аутентификации МОТО-транзакций. Такие технологии не обеспечивают решение на уровне инфраструктуры, на котором продавцы принимают данные аутентификации от держателей карт и передают такие данные эмитентам карт. Продавцам потребовались бы системы для приема и пересылки динамической информации. Кроме того, покупателям потребовались бы системы для передачи динамической информации эмитенту карты.

Соответственно держатели карт и продавцы обеспокоены частыми мошенническими МОТО-транзакциями и тем, что данные не являющихся мошенническими транзакций могут быть похищены в мошеннических целях. Существует потребность в способе и системе предотвращения несанкционированного доступа к МОТО-транзакциям.

Существует потребность в способе и системе, которая позволяет безопасно осуществлять МОТО-транзакцию.

Существует дополнительная потребность в способе и системе для осуществления двухфакторной аутентификации в МОТО-среде с целью предотвращения мошеннического доступа к МОТО-транзакции.

В основу настоящего изобретения положено решение одной или нескольких из перечисленных выше задач.

Краткое изложение сущности изобретения

Прежде чем приступить к описанию предложенных в изобретении способов, систем и материалов, следует отметить, что настоящее изобретение не ограничено конкретными описанными способами, системами и материалами, которые могут меняться. Также подразумевается, что используемая терминология имеет целью лишь описание конкретных вариантов осуществления, а не сужение объема изобретения, который ограничен лишь приложенной формулой изобретения.

Также следует отметить, что используемые в описании и формуле изобретения формы единственного числа включают множественное число, если только по контексту прямо не требуется иное. Так, например, термин "держатель карты"

обозначает одну или несколько сторон, участвующих в обмене ценностями, данными и/или информацией. Если только в прямой форме не указано иное, все не снабженные определениями научно-технические термины, используемые в описании, имеют значения, которые обычно подразумеваются специалистами в данной области техники, а значения всех снабженных определениями научно-технические термины считаются совпадающими со значениями, которые обычно подразумеваются специалистами в данной области техники. Хотя в изобретении применимы любые способы, материалы и устройства, подобные или эквивалентные тем, которые в нем описаны, далее описаны предпочтительные способы, материалы и устройства. Все упоминаемые в описании публикации включены в него порядке ссылки. Ничто в настоящем описании не следует толковать в качестве признания того, что изобретение предвосхищено каким-либо более ранним изобретением.

В одном из вариантов осуществления предложен способ аутентификации транзакции, связанной с заказами по почте и телефону, при осуществлении которого продавец принимает от держателя карты аутентификационную информацию, предоставляет аутентификационную информацию эмитенту, а эмитент определяет, является ли аутентификационная информация достоверной. Если аутентификационная информация является достоверной, эмитент может информировать продавца о том, что транзакция является законной. В противном случае эмитент может информировать продавца о том, что аутентификационная информация является недостоверной.

В одном из вариантов осуществления аутентификационная информация может содержать такую информацию, как одноразовый пароль, постоянный пароль, биометрические характеристики или любую иную информацию, которая может использоваться для аутентификации карты, счета или держателя карты. Например, такая информация может содержать звуковую информацию, звуковые биометрические характеристики, идентификационную бизнес-информацию, код страны, номер карточного счета, срок действия карты, имя держателя карты, задаваемые эмитентом данные аутентификации, указанные в данных "идентификатора банка-участника" (например, девичью фамилию матери), адрес для выставления счетов, адрес для доставки, номер социального страхования, номер телефона, сальдо счета, историю транзакции и/или номер водительского удостоверения.

В одном из вариантов осуществления эмитент может определять, инициировал ли продавец аутентификацию в ходе МОТО-транзакции.

В одном из вариантов осуществления эмитент может не предоставлять сообщение о личных гарантиях и/или иную информацию держателя карты, предоставленную держателем карты в ответ на аутентификационную информацию, если продавец передал информацию.

Краткое описание чертежей

Особенности, признаки, выгоды и преимущества вариантов осуществления настоящего изобретения станут ясны из следующего далее описания, приложенной формулы изобретения и чертежей, на которых:

на фиг.1 проиллюстрирован пример процесса регистрации держателя карты в службе аутентификации в одном из вариантов осуществления,

на фиг.2 показан пример процесса аутентифицированных платежных операций в одном из вариантов осуществления,

на фиг.3 показана блок-схема примерного процесса аутентификации МОТО-транзакции в одном из вариантов осуществления,

на фиг.4 показана блок-схема примерного процесса аутентификации МОТО-транзакции в одном из предпочтительных вариантов осуществления.

Описание изобретения

Далее описаны примеры способов организации, авторизации, регистрации и безопасного осуществления транзакций в среде для работы в реальном времени. Сначала может быть организована служба аутентификации. Организация службы аутентификации может включать осуществление процедур инициализации для каждого участника системы. Этими участниками может являться множество лиц, таких как продавцы, финансовые учреждения (т.е. эмитенты), покупатели и держатели карт. Продавцу, являющемуся клиентом службы аутентификации, может быть предоставлен сменный программный модуль, рассчитанный на среду для работы в реальном времени. В одном из вариантов осуществления сменный программный модуль может быть конкретно адаптирован к компьютерной платформе и программному обеспечению сервера электронной торговли продавца. Эмитенты-участники службы аутентификации могут предоставлять логотипы банков и маркетинговые образы для включения в специальный шаблон сайта регистрации в службе аутентификации. Покупатели также могут предоставлять продавцу корневой сертификат сертифицирующего органа обслуживающих организаций, сертификат протокола безопасных соединений сертифицирующего органа обслуживающих организаций для аутентификации клиентов и/или интеграционную поддержку.

До того как эмитент воспользуется службой аутентификации, эмитент может получить копию программно реализованных программ аутентификации, указанных в домене эмитента, и может установить системы аппаратного обеспечения и программное обеспечение службы аутентификации. Эмитенты также могут предоставлять службе аутентификации полисы аутентификации идентичности и идентификационный номер бизнес-участника (BIN, от английского - business identification number) для использования в ходе проверки держателя карты.

В одном из вариантов осуществления эмитент может предоставлять службе аутентификации аутентификационную информацию. Предварительная загрузка аутентификационной информации может облегчить крупномасштабную поддержку держателей карт. Например, когда эмитент желает активировать всех или почти всех своих держателей карт для службы аутентификации, эмитент может присвоить каждому держателю карты личный идентификационный номер (PIN, от английского - Personal Identification Number). После этого каждый держатель карты может использовать присвоенный ему PIN для доступа к аутентификационной информации. За счет этого можно ускорить процесс регистрации, поскольку от каждого держателя карты не требуется проходить формальный процесс регистрации.

Аутентификационная информация может содержать такую информацию, как динамический пароль, постоянный пароль, биометрические характеристики или любую иную информацию, которая может использоваться для аутентификации карты, счета или держателя карты. Например, такая информация может содержать звуковую информацию, звуковые биометрические характеристики, идентификационную бизнес-информацию, код страны, номер карточного счета, срок действия карты, имя держателя карты, задаваемые эмитентом данные аутентификации, указанные в данных "идентификатора банка-участника" (например, девичью фамилию матери), адрес для выставления счетов, адрес для доставки, номер социального страхования, номер телефона, сальдо счета, историю транзакции и/или номер водительского удостоверения. Эмитенты могут предоставлять серверу каталогов диапазоны номеров

счетов для своих портфелей карточных счетов и IP-адреса или унифицированные указатели ресурсов (URL, от английского - Uniform Resource Locators) станций управления доступом (ACS, от английского - access control server).

В одном из вариантов осуществления служба аутентификации может быть предложена через сайты банков, что позволяет держателям карт регистрироваться в службе аутентификации. В одном из альтернативных вариантов осуществления информация может передаваться по электронной почте, по телефону и/или посредством любого иного средства связи.

На фиг.1 проиллюстрирован пример процесса регистрации держателя карты в службе аутентификации в одном из вариантов осуществления. Как показано на фиг.1, на шаге 105 держатель карты может посетить регистрационный сайт, который поддерживает эмитент. В одном из альтернативных вариантов осуществления держатель карты может связаться с эмитентом по телефону, электронной почте и/или посредством любого иного средства связи. Держатель карты может зарегистрироваться в службе аутентификации, предоставив один или несколько номеров карточных счетов. На шаге 110 держатель карты может передать информацию, такую как основной номер счета (PAN, от английского - primary account number), имя держателя карты, срок действия карты, адрес, адрес электронной почты, опознавательный код покупателя, контрольный код счета, задаваемый держатель карты пароль и/или аутентификационную информацию.

После того как держатель карты передаст службе аутентификации запрошенную информацию, она может проверить, входит ли PAN держателя карты в диапазон номеров карт, зарегистрированных эмитентом. Служба аутентификации может дополнительно проверить идентичность держателя карты с использованием, например, базы данных аутентификации, которую поддерживает третье лицо и/или эмитент. В одном из вариантов осуществления эмитент может проверить идентичность держателя карты с использованием предоставленного эмитентом файла утвержденных держателей карт. В одном из вариантов осуществления эмитент может проверить идентичность держателя карты путем анализа авторизации контроля состояния. В одном из вариантов осуществления эмитент может проверить идентичность держателя карты путем сравнения ответов на информацию, предварительно загруженную в базу данных аутентификации, предоставленную эмитентом.

Если предоставленный PAN не входит в диапазон зарегистрированных эмитентом номеров карт, в регистрации может быть отказано, и процесс регистрации может быть завершен. Если PAN входит в диапазон зарегистрированных номеров карт через платежную сеть обслуживающей организации, такую как сеть VisaNet, для эмитента может быть осуществлена авторизации транзакции, например, на сумму в один доллар. В одном из вариантов осуществления авторизация транзакции на сумму в один доллар позволяет эмитенту проверить состояние карточного счета, проверить адрес с использованием службы проверки адресов и проверить контрольный код карты (CVV2). В процессе авторизации может быть проверена альтернативная или дополнительная информация. В одном из вариантов осуществления CVV2 может представлять собой трехзначное число, которое обычно напечатано с обратной стороны карты на строке для подписи.

Если карта является действительной, на шаге 115 служба аутентификации может запросить у держателя карты дополнительную аутентификационную информацию для проверки идентичности держателя карты. Держатель карты может ввести пароль и

пару "наводящий вопрос и ответ", чтобы аутентифицировать держателя карты при последующих транзакциях, связанных с покупками.

После того как идентичность держателя карты проверена и получены соответствующие ответы, на шаге 120 служба аутентификации может передать эмитенту сообщение об авторизации. Затем на шаге 125 сервер регистрации может передать информацию о держателе карты ACS, чтобы инициировать внесение записи в файл держателя счета. В файле держателя счета может храниться информация, такая как BIN финансовых учреждений, номера счетов, сроки действия, имена и фамилии, номера водительских удостоверений, адреса для выставления счетов, номера социального страхования, пароли держателей карт, вопросы-пароли держателей карт, ответы-пароли держателей карт, адреса электронной почты, показатели идентичности третьих лиц и другая информация.

После инициирования участников службы аутентификации и регистрации держателя карты может быть аутентифицирована платежная операция с использованием службы аутентификации.

На фиг.2 показан пример процесса аутентифицированных платежных операций в одном из вариантов осуществления. Как показано на фиг.2, держатель карты на шаге 205 может посетить сайт электронной торговли. После выбора товаров или услуг для приобретения держатель карты может начать процесс проверки, заполнить форму для проверки и на шаге 210 щелкнуть мышью по клавише "приобрести".

После выбора на шаге 210 клавиши "приобрести" может быть приведен в действие сменный программный модуль продавца. На шаге 215 сменный программный модуль продавца может осуществить проверку с целью определить, зарегистрирован ли указанный держателем карты счет в службе аутентификации. Проверка на шаге 215 может быть осуществлена с использованием i) процесса, в ходе которого проверяют сервер каталогов и ACS, связанные с держателем карты, ii) процесса, в ходе которого проверяют только ACS, и/или iii) процесса, в ходе которого продавец проверяет кэш-память, в которой хранится информация, аналогичная информации сервера каталогов.

Сменный программный модуль продавца может идентифицировать PAN и запросить сервер каталогов, чтобы проверить, входит ли PAN в диапазон номеров банка-эмитента, то есть участника службы аутентификации. Если счет не входит в диапазон PAN, заданных на сервере каталогов, служба аутентификации не регистрирует держателя карты. В этом случае продавец может быть уведомлен о том, что номер счета не зарегистрирован, и сменный программный модуль продавца может вернуть управление транзакцией программному обеспечению продавца для электронной торговли. После этого программное обеспечение продавца для электронной торговли может продолжить транзакцию, отказать держателю карты в дальнейшем обслуживании или перейти к альтернативным способам платежа.

Если PAN входит в диапазон PAN, известный серверу каталогов, он может передать PAN ACS, способному аутентифицировать держателя карты, чтобы определить, зарегистрирована ли карта. Если карта не зарегистрирована, процесс проверки может быть завершен. Если ACS сообщает, что карта зарегистрирована, ACS может через сервер каталогов сообщить свой URL сменному программному модулю продавца. Сменный программный модуль продавца может вызвать ACS через клиентское устройство держателя карты и его резидентный браузер. В службе аутентификации может храниться множество ACS.

В одном из вариантов осуществления сменный программный модуль продавца может запросить ACS, чтобы проверить, зарегистрирован ли держатель карты в

службе аутентификации. В одном из вариантов осуществления продавец может получить доступ к кэш-памяти, в которой хранится преимущественно такая же информация, что и на сервере каталогов, чтобы проверить, зарегистрирован ли держатель карты в службе аутентификации. В одном из вариантов осуществления сервер аутентификации может включать только один логический сервер каталогов, хотя в службе аутентификации может постоянно храниться несколько физических серверов каталогов.

Если держатель карты является участником службы аутентификации, ACS может отобразить для держателя карты окно с логотипом эмитента. В окне с логотипом эмитента может содержаться основная информация о платежной операции и запрос аутентификационной информации у держателя карты. Держатель карты может ввести аутентификационную информацию для ее проверки ACS.

Аутентификация платежа может быть продолжена, если немедленно введена правильная аутентификационная информация или дан правильный ответ на наводящий вопрос с использованием разрешенного числа попыток. ACS может поставить цифровую подпись на квитанции с использованием ключа подписи эмитента и/или поставщика услуг. В квитанции может быть указано имя продавца, номер карточного счета, сумма платежа и дата платежа. В файле квитанции может храниться имя продавца, URL продавца, номер карточного счета, срок действия, сумма платежа, дата платежа, подпись эмитента и/или контрольный код для аутентификации держателя карты. Затем ACS посредством браузера держателя карты может переадресовать держателя карты сменному программному модулю продавца и может передать ему снабженную цифровой подписью квитанцию и свое решение относительно того, был ли держатель карты аутентифицирован для продавца. Сменный программный модуль продавца может использовать сервер проверки достоверности, чтобы проверить цифровую. подпись, использованную для подписания квитанции об оплате. После проверки цифровой подписи держатель карты может считаться "аутентифицированным". По завершении транзакции держатель карты может перерегистрировать текущий карточный счет и/или создать новую аутентификационную информацию для использования в будущих транзакциях.

После аутентификации держателя карты может быть осуществлена авторизация указанного держателем карты счета. В частности, на шаге 220 продавец может передать через сменный программный модуль продавца платежной сети, такой как VisaNet сообщение об авторизации. Платежная сеть может переслать эмитенту сообщение об авторизации и индикатор электронной торговли (ECI, от английского - electronic commerce indicator). Эмитент может получить сообщение об авторизации и тем самым подтвердить продавцу, что по конкретному счету отсутствует задолженность и имеется соответствующий свободный лимит кредитования для запрошенной транзакции. В ECI может быть указано, что транзакция была осуществлена через Интернет с тем, чтобы можно было использовать соответствующий уровень защиты сообщения и аутентификации.

После того как эмитент осуществит обработку операции авторизации, управление операцией покупки может быть посредством платежной сети возвращено программному обеспечению продавца для электронной торговли. На шаге 225 эмитент может посредством платежной сети передать продавцу результат авторизации. Результатом авторизации может быть разрешение или отклонение транзакции.

В случае МОТО-транзакции продавец может инициировать аутентификацию

держателя карты путем переадресации держателя карты эмитенту для обмена аутентификационной информацией. Поскольку при MOTO-транзакции держатель карты не имеет прямой связи с эмитентом, держатель карты может предоставлять аутентификационную информацию продавцу. После этого продавец может предоставлять информацию от лица держателя карты. Соответственно при MOTO-транзакции продавец может выполнять функции, которые в случае транзакции с предъявлением карты или транзакции электронной торговли обычно выполняет держатель карты. В одном из вариантов осуществления аутентификационная информация может генерироваться динамически, чтобы предотвратить мошенническое использование аутентификационной информации продавцом и иное нарушение защиты. Система транзакций может определять, вводит ли информацию продавец, а не держатель карты, путем запроса информации у продавца. Соответственно при осуществлении MOTO-транзакции продавцу может не передаваться конфиденциальная информация держателя карты информация, такая как сообщение о личных гарантиях. В одном из вариантов осуществления используют идентификатор, который может указывать, осуществлена ли MOTO-транзакция.

Когда продавец действует от лица держателя карты при осуществлении MOTO-транзакции, осуществление некоторых функций может быть неуместным. Например, при обработке MOTO-транзакции могут быть заблокированы функциональные возможности, позволяющие держателю карты генерировать аутентификационную информацию во время транзакции с целью проверки держателя карты при будущих транзакциях. Это может быть неуместным, когда ввод данных при транзакции осуществляет продавец. Аналогичным образом, если эмитент отслеживает местоположение инициатора транзакция с целью уменьшения риска, такие функциональные возможности могут быть заблокированы при осуществлении MOTO-транзакции, в ходе которой продавец вводит аутентификационную информацию.

На фиг.3 показана блок-схема примерного процесса аутентификации MOTO-транзакции в одном из вариантов осуществления. Как показано на фиг.3, держатель карты может выбирать наименования из каталога и на шаге 305 окончательно оформлять покупку, например, по телефону или электронной почте. На шаге 310 продавец может передать, например, серверу каталогов запрос регистрации покупки. В запрос регистрации может быть включен индикатор MOTO-транзакции. Индикатор может указывать, что транзакция является MOTO-транзакцией и что держатель карты не будет непосредственно предоставлять аутентификационную информацию. Если номер карты, сообщенный держателем карты продавцу и переданный серверу каталогов, находится в диапазоне 315 номеров карт-участников, сервер каталогов на шаге 320 может передать запрос регистрации, например, соответствующему ACS. На шаге 325 ACS может передать серверу каталогов ответ на запрос регистрации с указанием того, доступна ли аутентификация для карты. Если номер карты не входит в диапазон номеров карт-участников, на шаге 330 сервер каталогов может создать ответ на запрос регистрации, отклоняющий транзакцию. На шаге 335 ответ на запрос регистрации может быть передан продавцу.

Если допустить, что аутентификация доступна, на шаге 340 продавец через браузер продавца может передать ACS запрос аутентификации. На шаге 345 ACS может принять запрос аутентификации и на шаге 350 аутентифицировать держателя карты применительно к номеру карты. Например, от держателя карты может потребоваться предоставить аутентификационную информацию, криптограмму чипа, PIN и/или т.п. ACS может определять, что транзакция является MOTO-транзакцией путем сравнения

идентификатора счета держателя карты с запросом регистрации. ACS может дополнительно определять, какие поля информации держателя карты информация не являются конфиденциальными для держателя карты и тем самым могут быть отображены для продавца. Например, может быть неуместным отображать для продавца сообщение о личных гарантиях. ACS может форматировать и снабжать цифровой подписью ответное сообщение на запрос аутентификации перед его передачей на шаге 355 продавцу через браузер продавца. В одном из вариантов осуществления ACS может передавать ответ на запрос аутентификации серверу истории аутентификации для будущей проверки. На шаге 360 продавец может принимать ответ на запрос аутентификации и на шаге 365 проверять подлинность подписи на ответе на запрос аутентификации. Если подлинность установлена, на шаге 370 продавец может дать согласие на осуществление транзакции с покупателем.

В одном из вариантов осуществления держателю карты может быть предоставлен динамический способ генерирования аутентификационной информации. Способ, которым генерируют аутентификационную информацию, может меняться и может быть в прямой форме не ограничен в настоящем описании. Например, держателю карты может быть предоставлен напечатанный перечень одноразовых паролей и/или паролей с ограниченным сроком действия. Держателю карты также может быть предоставлено устройство для ввода одноразовых паролей, карта и/или считывающее устройство, генерирующее одноразовый пароль, и/или карта, в которой для генерирования одноразового пароля используются биометрические характеристики.

В качестве усовершенствования предшествующих способов осуществления MOTO-транзакций может быть предусмотрена возможность аутентификации держателя карты без внесения значительных изменений в базовую систему транзакций, используемую в среде электронной торговли и/или банковских операций в оперативном режиме. Описанная в изобретении MOTO-транзакция как таковая способна улучшить защиту без внесения существенных изменений в базовую инфраструктуру.

В одном из вариантов осуществления может использоваться постоянный пароль. Это может обеспечить дополнительное удобство держателю карты. В одном из вариантов осуществления постоянные пароли могут использоваться в MOTO-транзакциях, в которых держатель карты предоставляет пароль непосредственно эмитенту, а не продавцу.

На фиг.4 показана блок-схема примерного процесса аутентификации MOTO-транзакции в одном из предпочтительных вариантов осуществления. Как показано на фиг.4, на шаге 405 оператор MOTO-транзакции может от лица клиента выполнить одну или несколько функций с использованием корзины для виртуальных покупок на сайте продавца. В одном из вариантов осуществления одной или несколькими функциями может одна являться одна или несколько функций, включающих выбор товара, увеличение, уменьшение и/или обновление количеств товара и учет текущего общего количества выбранного товара. Затем на шаге 410 оператор MOTO-транзакции может осуществить процесс проверки. Например, оператор MOTO-транзакции может от лица клиента ввести информацию о доставке, информация об оплате и/или окончательно оформить транзакцию.

В одном из вариантов осуществления после этого может быть инициирован процесс проверки. Например, на шаге 415 сменный программный модуль продавца может передать ACS эмитента запрос проверки регистрации (VEReq). В одном из вариантов осуществления VEReq может содержать индикатор MOTO-транзакции, установленный

в положение MOTO-транзакции. Индикатор MOTO-транзакции может указывать, что транзакция является MOTO-транзакцией и тем самым, что держатель карты не будет непосредственно предоставлять аутентификационную информацию. На шаге 420 ACS может определять, установлен ли индикатор MOTO-транзакции в положение VEReq. Если это так, на шаге 425 ACS может передать оператору MOTO-транзакции ответ на запрос проверки регистрации (VERes), адаптированный к MOTO-транзакции. В одном из вариантов осуществления VERes может содержать информацию, указывающую, доступна ли аутентификация для транзакции.

Если аутентификация доступна для карты, на шаге 430 оператор MOTO-транзакции может через браузер продавца передать ACS запрос аутентификации плательщика (PAReq). На шаге 435 ACS может принять PAReq и на шаге 440 соответствующим образом аутентифицировать держателя карты, исходя из номера карты. В одном из вариантов осуществления ACS может распознавать идентификатор счета в качестве MOTO-транзакции, исходя из описанного выше процесса VEReq/VERes. Затем на шаге 445 ACS может генерировать ответ на запрос идентификации плательщика (PARes) для передачи оператору MOTO-транзакции. В одном из вариантов осуществления в случае MOTO-транзакции ACS может не передавать конфиденциальную информацию держателя карты, такую как сообщение о личных гарантиях, пароль и/или т.п. В одном из вариантов осуществления в случае MOTO-транзакции ACS может блокировать функцию активирования во время совершения покупок, служащую для слежения за местом осуществления покупок клиентом с целью обнаружения мошенничества. На шаге 450 оператор MOTO-транзакции может получать PARes и необязательно отображать информацию, касающуюся транзакции, которую аутентифицирует эмитент. Затем оператор MOTO-транзакции может приступить к процессу авторизации транзакции, в ходе которой оператору MOTO-транзакции обычным способом переводят денежную сумму.

Подразумевается, что различные из описанных выше признаков и функций или их альтернатив могут быть, по желанию, объединены во множество других отличающихся систем или программ. Также подразумевается, что специалисты в данной области техники могут впоследствии включить в изобретение различные непредусмотренные или непредвиденные в изобретении альтернативы, модификации, варианты или усовершенствования.

Формула изобретения

1. Способ аутентификации, при осуществлении которого:

продавец вводит в систему продавца:

заказ по почте или телефону (MOTO) и данные карты, которую держатель карты использует для транзакции, содержащие номер карты для транзакции и аутентификационную информацию, предоставленную держателем карты, при этом данные MOTO и данные карты для транзакции принимают по электронной почте или по телефону, с помощью системы продавца передают серверу аутентификации запрос проверки регистрации, содержащий номер карты для транзакции и индикатор, указывающий, что: запрос проверки регистрации относится к транзакции, и аутентификационная информация, предоставленная держателем карты, не будет передана держателем карты, с помощью системы продавца принимают от сервера аутентификации ответ на запрос проверки регистрации, в котором указано, доступна ли аутентификация карты для транзакции, по меньшей мере, на основании номера карты для транзакции, и если аутентификация карты доступна: с помощью системы

продавца принимают от сервера аутентификации предложение об аутентификации, в котором не содержится или не запрашивается конфиденциальная информация держателя карты, которая содержит подтверждение достоверности персональной информации или пароль, с помощью системы продавца вводят аутентификационную информацию, предоставленную держателем, в предложение об аутентификации, при этом аутентификационная информация формируется картой транзакции, с помощью системы продавца передают серверу аутентификации запрос аутентификации, содержащий аутентификационную информацию, предоставленную держателем карты, и с помощью системы продавца принимают от сервера аутентификации ответ на запрос аутентификации, в котором указано, аутентифицирован ли держатель карты.

2. Способ по п.1, в котором ответ на запрос аутентификации снабжен цифровой подписью сервера аутентификации.

3. Способ по п.2, при осуществлении которого дополнительно проверяют достоверность подписи ответа на запрос аутентификации.

4. Способ по п.1, в котором для формирования аутентификационной информации в карте для транзакции используются биометрические характеристики.

5. Способ по п.1, в котором аутентификационная информация содержит одноразовый пароль.

6. Способ по п.1, в котором транзакцию не авторизуют, если держатель карты не аутентифицирован.

7. Способ аутентификации транзакции, в котором: аутентифицируют карту транзакции, используемую при осуществлении заказа по почте или телефону (MOTO), для чего: с помощью сетевого устройства, обменивающегося данными с системой продавца, принимают от системы продавца запрос проверки регистрации, содержащий номер карты для транзакции и индикатор, указывающий, что: запрос проверки регистрации касается MOTO-транзакции и аутентификационная информация, предоставленная держателем карты, не будет передана держателем карты, с помощью сетевого устройства передают системе продавца ответ на запрос проверки регистрации, в котором указано, доступна ли аутентификация по меньшей мере на основании номера карты для транзакции, и аутентифицируют держателя карты с целью осуществления MOTO-транзакции, для чего: если аутентификация карты доступна: с помощью сетевого устройства принимают от системы продавца запрос аутентификации, с помощью сетевого устройства передают системе продавца предложение об аутентификации, в котором не содержится или не запрашивается конфиденциальная информация держателя карты, которая содержит подтверждение достоверности персональной информации или пароль, с помощью сетевого устройства принимают аутентификационную информацию, предоставленную держателем карты и введенную продавцом с помощью системы продавца в предложение об аутентификации, при этом аутентификационная информация динамично сформирована картой транзакции, и с помощью сетевого устройства передают системе продавца ответ на запрос аутентификации, в котором указано, аутентифицирован ли держатель карты.

8. Способ по п.7, в котором ответ на запрос аутентификации снабжен цифровой подписью.

9. Способ по п.7, в котором для динамичного формирования аутентификационной информации в карте для транзакции используются биометрические характеристики.

10. Способ по п.8, в котором аутентификационная информация содержит одноразовый пароль.

11. Способ по п.7, в котором транзакцию авторизуют.

12. Способ по п.7, в котором транзакцию не авторизуют, если держатель карты не аутентифицирован.

13. Способ аутентификации в ходе осуществляемой в реальном времени платежной операции с использованием карты для транзакции в платежной системе, включающей систему продавца и сервер аутентификации, в котором:

вводят в систему продавца: заказ по почте или телефону (МОТО) и данные карты для транзакции, содержащие номер карты для транзакции, при этом данные МОТО и данные карты для транзакции принимают по электронной почте или по телефону, с помощью системы продавца передают серверу аутентификации запрос проверки регистрации, содержащий номер карты для транзакции и индикатор, указывающий, что запрос проверки регистрации касается МОТО-транзакции, с помощью системы продавца принимают от сервера аутентификации ответ на запрос проверки регистрации, в котором указано, доступна ли аутентификация карты транзакции по меньшей мере на основании номера карты для транзакции, и

если аутентификация карты доступна:

с помощью системы продавца передают серверу аутентификации запрос аутентификации, с помощью системы продавца принимают от сервера аутентификации предложение об аутентификации, в котором не содержится или не запрашивается конфиденциальная информация держателя карты, которая содержит подтверждение достоверности персональной информации или пароль, в ответ на предложение об аутентификации с помощью системы продавца передают держателю карты сообщение о переадресации держателя карты на эмитента карты для транзакции с целью получения аутентификационной информации для аутентификации держателя карты, с помощью системы продавца принимают от эмитента аутентифицированную информацию, полученную эмитентом от держателя карты, с помощью системы продавца передают серверу аутентификации запрос аутентификации, с помощью системы продавца принимают от сервера аутентификации ответ на запрос аутентификации, в котором указано, аутентифицирован ли держатель карты, и если держатель карты аутентифицирован:

с помощью системы продавца передают платежной сети запрос авторизации и индикатор, указывающий, что запрос регистрации касается транзакция в системе электронной торговли, и с помощью системы продавца принимают от платежной сети результат авторизации, в котором указано, авторизован ли счет, соответствующий карте.

14 Способ по п.13, в котором запрос аутентификации содержит номер карты.

15. Способ по п.13, в котором для динамичного формирования аутентификационной информации в карте для транзакции используются биометрические характеристики.

16. Способ по п.13, в котором аутентификационная информация содержит одноразовый пароль.

17. Способ по.13, в котором при авторизации осуществляемой в реальном времени платежной операции в соответствии с ответом на запрос авторизации с помощью системы продавца передают запрос авторизации эквайеру продавца, относящегося к системе продавца.

18. Способ по п.13, в котором транзакцию не авторизуют, если держатель карты не аутентифицирован.

19. Способ по п.1, в котором в запросе проверки регистрации указано, что

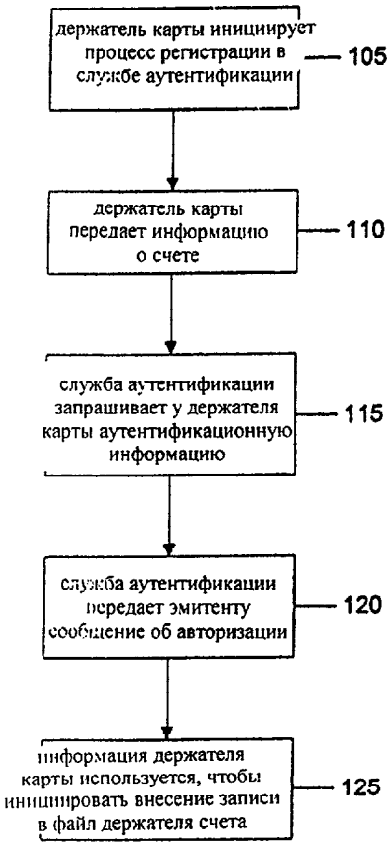
аутентификация доступна, если номер используемой для транзакции карты находится в предварительно заданном интервале.

20. Способ по п.19, в котором в запросе проверки регистрации указано, что в аутентификации отказано, если номер карты не находится в предварительно заданном интервале.

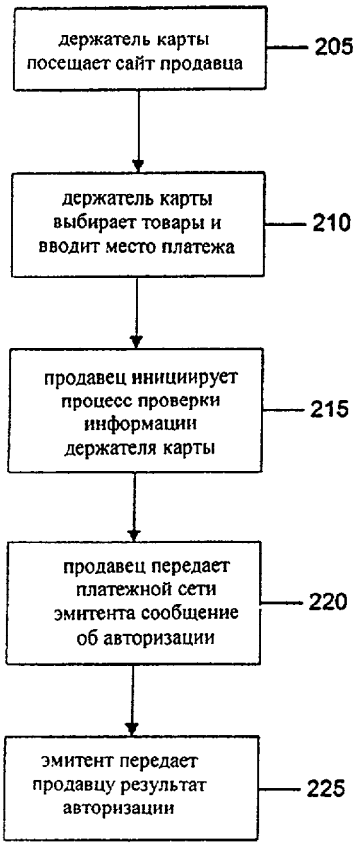
21. Способ по п.3, в котором проверка достоверности подписи ответа на запрос аутентификации позволяет системе продавца авторизовать МОТО транзакцию в системе эквайера.

22. Способ по п.7, в котором при осуществлении МОТО транзакции блокируются функциональные возможности, позволяющие держателю карты генерировать аутентификационную информацию для проверки держателя карты при осуществлении будущей транзакции.

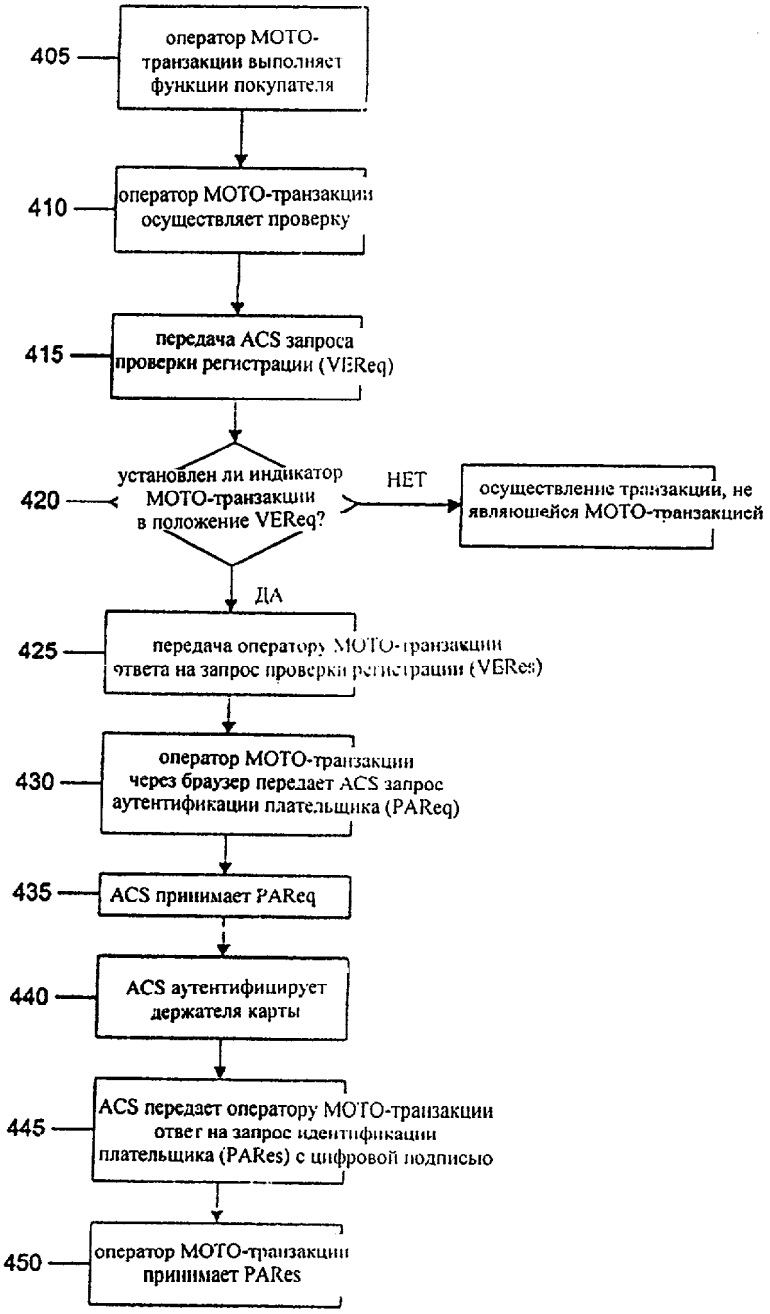
23. Способ по п.13, в котором при осуществлении МОТО транзакции блокируются функциональные возможности, позволяющие эмитенту отслеживать местонахождение держателя карты.


держатель карты инициирует процесс регистрации в службе аутентификации
105
держатель карты передает информацию о счете
110
служба аутентификации запрашивает у держателя карты аутентификационную информацию
115
служба аутентификации передает эмитенту сообщение об авторизации
120
информация держателя карты используется, чтобы инициировать внесение записи в файл держателя счета
125

Фиг. 1


держатель карты посещает сайт продавца
205
держатель карты выбирает товары и вводит место платежа
210
продавец инициирует процесс проверки информации держателя карты
215
продавец передает платежной сети эмитента сообщение об авторизации
220
эмитент передает продавцу результат авторизации
225

Фиг. 2


405
оператор МОТО-транзакции выполняет функции покупателя
410
оператор МОТО-транзакции осуществляет проверку
415
передача ACS запроса проверки регистрации (VEReq)
420
установлен ли индикатор МОТО-транзакции в положение VEReq?
НЕТ
осуществление транзакции, не являющейся МОТО-транзакцией
ДА
425
передача оператору МОТО-транзакции ответа на запрос проверки регистрации (VERes)
430
оператор МОТО-транзакции через браузер передает ACS запрос аутентификации плательщика (PAReq)
435
ACS принимает PAReq
440
ACS аутентифицирует держателя карты
445
ACS передает оператору МОТО-транзакции ответ на запрос идентификации плательщика (PARes) с цифровой подписью
450
оператор МОТО-транзакции принимает PARes

Фиг. 4