РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 292 589** (13) **C2**

(51) МПК
G06Q 30/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2002130717/09, 17.04.2001**

(24) Дата начала отсчета срока действия патента:
17.04.2001

(30) Конвенционный приоритет:
17.04.2000 (пп.1-14) US 60/198,110

(43) Дата публикации заявки: **10.03.2004**

(45) Опубликовано: **27.01.2007 Бюл. № 3**

(56) Список документов, цитированных в отчете о поиске: **US 5793028 A, 11.08.1998. RU 2136042 C1, 27.08.1999. US 5905248 A, 18.05.1999. US 5991413 A, 23.11.1999. WO 99/42961 A1, 26.08.1999. WO 97/49052 A1, 24.12.1997. Норенков В.А. и др. Телекоммуникационные технологии и сети, Москва, МГТУ имени Н.Э.Баумана, 1998, стр.153.**

(85) Дата перевода заявки PCT на национальную фазу:
18.11.2002

(86) Заявка PCT:
US 01/12445 (17.04.2001)

(87) Публикация PCT:
WO 01/78493 (25.10.2001)

Адрес для переписки:
129010, Москва, ул. Б. Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Автор(ы):
ГРЭЙВС Майкл Е. (US),
ФРЭНК Питер Е. (US),
ПЛЭМБЕК Тэйн (US),
УАЙТХЕД Грегори Р. (US)

(73) Патентообладатель(и):
ВЕРИСАЙН, ИНК. (US)

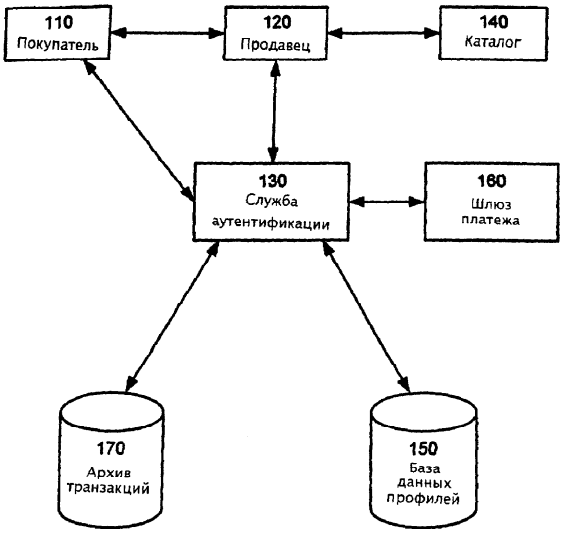
RU 2292589 C2

(54) АУТЕНТИФИЦИРОВАННЫЙ ПЛАТЕЖ

(57) Реферат:

Изобретение относится к аутентификации покупателей при осуществлении интерактивных коммерческих транзакций. Техническим результатом является обеспечение защиты от несанкционированного доступа. В системе и способе покупатель предпочитает использовать средство электронных платежей как часть коммерческой транзакции с продавцом, осуществляемой в интерактивном режиме, при этом требуется аутентифицировать наличие у покупателя полномочий использовать средство платежей. Отдельная служба аутентификации выполнена на WEB-сервере и предназначена для определения, имеет ли покупатель доступ к некоторой секретной информации без раскрытия секретной информации продавцу. Служба аутентификации информирует продавца, имеет ли покупатель полномочия использовать средство платежей. При идентификации покупателя используют данные о профиле покупателя, включающем данные о множестве инструментов платежа и адресов отгрузки, которые использует покупатель. 2 н. и 12 з.п. ф-лы, 9 ил.

RU 2292589 C2



Фиг. 1

RU 2292589 C2

RU 2292589 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 292 589** (13) **C2**

(51) Int. Cl.
G06Q 30/00 (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2002130717/09, 17.04.2001**

(24) Effective date for property rights: **17.04.2001**

(30) Priority:
17.04.2000 (cl.1-14) US 60/198,110

(43) Application published: **10.03.2004**

(45) Date of publication: **27.01.2007 Bull. 3**

(85) Commencement of national phase: **18.11.2002**

(86) PCT application:
US 01/12445 (17.04.2001)

(87) PCT publication:
WO 01/78493 (25.10.2001)

Mail address:
129010, Moskva, ul. B. Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor(s):
GREhJVS Majkl E. (US),
FREhNK Piter E. (US),
PLEhMBEK Tehjn (US),
UAJTKhED Gregori R. (US)

(73) Proprietor(s):
VERISAJN, INK. (US)

(54) AUTHENTIFIED PAYMENT

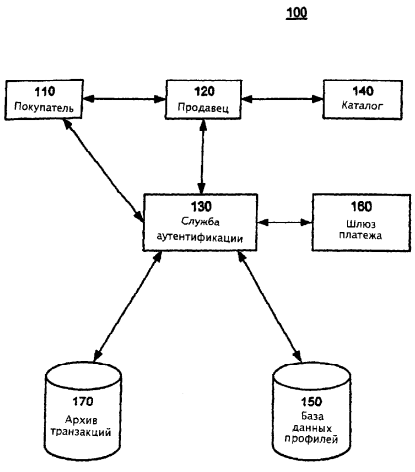
(57) Abstract:

FIELD: authentication of buyers during realization of interactive commercial transactions.

SUBSTANCE: in the system and method buyer prefers using means of electronic payment, as part of commercial transaction with seller, performed in interactive mode, while it is required to authenticate privileges of client for usage of payment means. Separate authentication service is made on WEB-server and is meant for determining whether buyer has access to certain secret information without revealing secret information to seller. Authentication service informs the seller whether buyer has privileges to use payment means. During identification of buyer, buyer profile data are used, including data about multiple payment tools and delivery addresses used by buyer.

EFFECT: provision of protection from unsanctioned access.

2 cl, 9 dwg



Фиг. 1

RU 2292589 C2

RU 2292589 C2

Данная заявка испрашивает приоритет предварительной заявки на патент США, регистрационный номер 60/198.110, называемой "Аутентифицированный платеж", поданной 17 апреля 2002 года на имя Greg Whitehead, Michael Graves, Thane Plambeck.

Область техники

Настоящее изобретение относится к аутентификации покупателей при осуществлении интерактивных коммерческих транзакций и, более конкретно, к использованию отдельной службы аутентификации, осуществляющей аутентификацию покупателя.

Предшествующий уровень техники

В результате роста популярности и использования Интернета и других форм сетевой связи широко применяется интерактивная коммерция (коммерция в режиме реального времени). Например, постоянно увеличивается объем покупок пользователей, торговых операций между торгово-промышленными предприятиями, продажа акций и другие формы вложения капитала, осуществляемые через Интернет и/или беспроводные сети связи, и другие формы интерактивной коммерции. Кроме того, для использования преимуществ уникальных свойств интерактивной коммерции значительные усилия прилагаются для разработки альтернативных бизнес-моделей (например, аукционов и оптовых покупок) и альтернативных форм электронного платежа (например, электронного наличного расчета и авторизованных переводов денежных средств через Интернет).

Однако одним из недостатков интерактивной коммерции является сложность аутентификации покупателя. Примером может служить случай, когда пользователь предпочитает приобрести товар с использованием кредитной карточки. При приобретении товара в реальном мире от покупателя требуется предъявить свою кредитную карточку (возможно, имеющую фотографию) и подписать бланк кредитной карточки подписью, соответствующей подписи на кредитной карточке. Эти действия выполняют две важные задачи. Во-первых, они с определенной достоверностью устанавливают, что покупатель имеет полномочия использовать кредитную карточку. Во-вторых, они формируют запись, которая затрудняет отрицание покупателем впоследствии того, что он санкционировал покупку. Эти два фактора значительно уменьшают риск мошеннической транзакции.

В интерактивном варианте данной транзакции действия, которые соответствуют предъявлению кредитной карточки и подписанию бланка кредитной карточки, или не существуют, или, если они существуют, то не так эффективны в смысле уменьшения риска. Например, во многих случаях от покупателя требуется просто напечатать номер своей кредитной карточки и затем щелкнуть кнопку Осуществить Покупку. Эти два действия допускают мошенничество в большей степени, чем их аналоги в реальном мире, поскольку продавец не знает, действительно ли человек, предпринимающий эти действия, имеет полномочия использовать эту кредитную карточку. Другими словами, продавцу сложно аутентифицировать покупателя. Дополнительно, даже если транзакция санкционирована истинным владельцем кредитной карточки, то повышенный риск мошенничества означает, что полученная в результате запись не имеет юридического значения, поскольку владелец кредитной карточки может утверждать, что транзакцию санкционировал самозванец. Этот дополнительный риск мошенничества в ситуации "карточка не представлена" приводит к более высоким тарифам взаимного обмена и плате за транзакции, обрабатываемые через Интернет и другие системы интерактивной коммерции, и, возможно, обеспечивает наибольшую составляющую стоимости коммерции через Интернет.

Одной из причин роста мошенничества при использовании Интернета и роста другого электронного мошенничества является то, что личная информация средств платежа, например номера кредитных карточек, номера контрольных счетов, и связанные с ними данные стали по существу "информацией общего пользования" в том смысле, что эти данные легко доступны. Например, пользователь в незащищенном формате передает номер своей кредитной карточки, дату конечного срока и т.д. каждому электронному продавцу при каждой транзакции. Дополнительно такая информация, как имя, адрес, номер социального страхования и т.д. также является доступной из других источников, отличных от держателя карточки. Например, много информации такого вида может

содержаться в телефонных каталогах и каталогах другого вида, доступных для просмотра средствами Web. Информация средств платежа, которая приводится в незащищенном виде и повторяется, совместно с тем фактом, что многое из этой информации также является доступным из других источников, увеличивает риск мошеннических транзакций. Например, хакерам зачастую необходимо только захватить базы данных номеров кредитных карточек и информацию соответствующих им имен и адресов, чтобы во многих средах осуществления интерактивных транзакций подменить фактического держателя карточки.

Обычно проблема аутентификации покупателя решалась посредством использования паролей, что представляет собой подход, стандартно используемый в коммерческих средах Интернета (Web), где покупатель аутентифицирует себя, используя просто имя пользователя и пароль. Как описано выше, пароли имеют свойственные им недостатки и при использовании для этой цели нынешние реализации еще более усугубляют эти недостатки. Например, обычно пользователи должны регистрироваться индивидуально каждым электронным продавцом, использующим интерактивный процесс. В результате электронный продавец имеет ограниченную возможность подтвердить регистрацию пользователя, поскольку время интерактивной регистрации часто не позволяет осуществить существенную проверку, и даже если имеется возможность осуществить такую проверку, то препятствовать будет оплата, поскольку каждый электронный продавец должен сам оплачивать осуществляемую им проверку. Дополнительно пользователи часто используют одни и те же имена пользователя и пароли для нескольких учетных записей. Это увеличивает возможность подвергнуть риску имя пользователя и пароль, и если они подверглись риску, то увеличивает потенциально возможный ущерб. Дополнительно, поскольку имя пользователя и пароль обычно передаются электронному продавцу незащищенным текстом, то недобросовестные электронные продавцы могут также использовать эту информацию, чтобы подвергнуть риску другие учетные записи пользователя. В качестве последнего примера можно отметить, что многие существующие системы аутентификации аутентифицируют идентичность пользователя (например, подтверждая, что пользователь действительно является Джоном До), но аутентификация идентичности кого-то не обязательно является подтверждением того, что этот кто-то имеет полномочия использовать конкретное средство платежа.

Одной из попыток решить проблему аутентификации покупателя, содействующей осуществлению через Интернет защищенных транзакций с использованием платежных карточек, является протокол Защищенных электронных транзакций (или ЗЭТ). В ЗЭТ использовались цифровые сертификаты для образования достоверной последовательности в ходе транзакции. Например, пользователь должен иметь цифровой сертификат, который он предъявляет электронному продавцу. Электронный продавец должен иметь цифровой сертификат, который он предъявляет пользователю. Для обеспечения достоверности каждый должен проверить цифровой сертификат другого и основную последовательность цифровых сертификатов. Однако этот подход вносит значительное административное и операционное усложнение для пользователей, для электронных продавцов и в соответствующую инфраструктуру обработки транзакций. Например, покупателям и электронным продавцам для использования протокола требуется специализированная технология, и они будут вынуждены обновлять технологию при каждом принятии новых цифровых сертификатов. В результате протокол ЗЭТ не получил широкого распространения.

Следовательно, существует потребность в существенной аутентификации покупателя при интерактивных коммерческих транзакциях. Дополнительно существует потребность в способе аутентификации покупателя, который является достаточно гибким для обеспечения возможности разного уровня защиты для разных приложений и также для принятия новых технологий. Также предпочтительно, чтобы способ не вносил значительных трудностей в существующую инфраструктуру обработки транзакций или не требовал ее сильной модификации.

Сущность изобретения

Согласно настоящему изобретению интерактивная система (100) коммерческих транзакций содержит покупателя (110), продавца (120) и службу (130) аутентификации. Для продавца (120) требуется аутентифицировать (204), что покупатель (110) имеет полномочия использовать средство платежа как часть интерактивной коммерческой транзакции с продавцом (120). Для этого служба (130) аутентификации выполняет следующие этапы, которые осуществляются в режиме реального времени, как часть интерактивной коммерческой транзакции. Служба (130) аутентификации принимает (230) запрос на подтверждение наличия у покупателя (110) полномочий использовать средство платежа.

Она определяет (246), имеет ли покупатель (110) доступ к некоторой секретной информации без раскрытия секретной информации продавцу (120). Доступ к секретной информации должен подтвердить наличие полномочий на использование средства платежа. В зависимости от определения, имеет ли покупатель (110) доступ к секретной информации, служба (130) аутентификации передает (250) продавцу (120) ответ, содержащий информацию о том, имеет ли покупатель (110) полномочия использовать средство платежа. Согласно другому аспекту изобретения служба (130) аутентификации также применяет (260) информацию с личными данными (информацию профиля) покупателя (110) в интерактивную коммерческую транзакцию и/или обрабатывает (270) или по меньшей мере частично обрабатывает транзакцию платежа. Служба (130) аутентификации также может хранить (280) запись об использовании средства платежа и/или о транзакции.

В предпочтительном варианте осуществления (300) интерактивная коммерческая транзакция осуществляется через Интернет. Покупатель (110) осуществляет доступ к Интернету через средство просмотра Web (Web-браузер), продавец (120) использует электронную витрину Интернет, размещенную на Web сервере, и служба (130) аутентификации реализуется на Web сервере. Дополнительно секретная информация содержит секретный ключ. Другими словами, создание цифровых подписей, использующих секретный ключ, должно являться доказательством того, что подписывающееся лицо имеет полномочия использовать соответствующее средство платежа. В этом варианте осуществления запрос (330) на аутентификацию инициируется представлением покупателем формы (400), которая содержит активный элемент, идентифицирующий службу (130) аутентификации. Запрос (330) в службу (130) аутентификации также содержит адрес продавца, чтобы служба аутентификации имела информацию о том, куда передать (350) результаты процесса аутентификации. Для аутентификации продавца (120) служба (130) аутентификации передает (340) запрос покупателю (110), требующий, чтобы покупатель (110) использовал секретный ключ для подписи цифровой подписью некоторых данных. Служба (130) аутентификации использует ответ (342) покупателя для определения (346), имеет ли покупатель (110) доступ к секретному ключу, и затем передает (350) результаты продавцу (120). Служба (130) аутентификации может запросить у покупателя (110) дополнительно подписать цифровой подписью запись транзакции, создавая (380), таким образом, строгую запись транзакции (имеющую юридическое значение).

Настоящее изобретение имеет особенное преимущество, поскольку для аутентификации покупателя (110) используется отдельная служба (130) аутентификации, а не продавец (120). В результате продавец (120) не получает доступ к секретной информации, связанной со средством платежа покупателя. Это предотвращает повторное использование секретной информации продавцом (120) для санкционирования впоследствии мошеннических транзакций.

Дополнительно сосредоточение функции аутентификации в службе (130) аутентификации приводит к значительной гибкости и снижению расходов на масштабирование системы. Могут быть использованы различные виды секретной информации, причем каждый вид для своей реализации требует отличающейся технологии. Сосредоточение функции аутентификации в службе (130) аутентификации

позволяет разделить стоимость требуемой технологии на многих продавцов (120). Дополнительно при изменении вида секретной информации или соответствующей процедуры аутентификации покупателя большая часть изменений повлияет только на службу (130) аутентификации (130), следовательно, легко обеспечивается реализация новых технологий аутентификации. Если служба (130) аутентификации выполняет другие функции, такие как добавление к транзакции информации профиля покупателя, обработку средства платежа или создание и хранение записей транзакций, то может быть произведено дополнительное снижение расходов на масштабирование, поскольку служба (130) аутентификации естественным образом является централизованным пунктом для этих других функций.

Краткое описание чертежей

Описанные выше и другие более детализированные и конкретные задачи и свойства настоящего изобретения раскрыты более полно в последующем описании, иллюстрируемом чертежами, на которых представлено следующее:

фиг.1 - блок-схема системы, соответствующей настоящему изобретению;

фиг.2 - запись событий, иллюстрирующая способ функционирования системы, изображенной на фиг.1;

фиг. 3 - запись событий, иллюстрирующая предпочтительный способ функционирования предпочтительного варианта осуществления системы, изображенной на фиг.1;

фиг. 4-7 - разные экранные изображения и диалоговые окна, иллюстрирующие способ, представленный на фиг. 3.

Подробное описание предпочтительных вариантов осуществления

На фиг.1 изображена блок-схема системы 100 согласно настоящему изобретению. Система 100 содержит покупателя 110, продавца 120 и службу 130 аутентификации, связанные друг с другом. Система 100 также может содержать каталог 140 служб аутентификации, который является доступным для покупателя 110, и базу данных 150 профилей покупателей и архив 170 транзакций, которые доступны для службы 130 аутентификации. Необязательный шлюз 160, используемый для осуществления платежа, (шлюз платежа) также доступен для службы 130 аутентификации, хотя в альтернативных вариантах осуществления доступ к шлюзу 160 платежа может иметь продавец 120 или служба 130 аутентификации и продавец 120. Шлюз 160 платежа является просто каналом, через который передаются к соответствующим финансовым учреждениям транзакции платежа. Настоящее изобретение может использоваться с многими разными видами шлюзов 160 платежа (или даже без шлюза платежа) и не ограничено использованием конкретного вида технологии шлюзов.

Покупатель 110 предпочитает использовать средство платежа как часть интерактивной коммерческой транзакции с продавцом 120. Например, в одном приложении покупателем 110 является пользователь, продавцом 120 является электронныйпродавец с электронной витриной в Интернете, и пользователь для покупки у электронного продавца некоторого продукта, информации или услуги предпочитает использовать свою кредитную карточку. В качестве другого возможного варианта покупателем 110 является индивидуальное лицо, соединяющееся с продавцом 120 через радиотелефон или карманный персональный цифровой ассистент (ПЦА), продавцом 120 является служба оплаты счетов, и для упомянутого лица предпочтительно выписать "Интернет-чеки" для оплаты своих ежемесячных счетов. В качестве другого возможного варианта покупателем 110 является корпорация или лицо, действующее от имени корпорации, покупающее материалы или услуги у поставщика 120 корпорации. Другие возможные варианты средств платежа включают текущие номера контрольного счета, виртуальные деньги или электронные представления наличных, значение денежной предоплаты, которое хранится в электронных бумажниках, платежные карточки и кредиты или купоны Интернета.

Из рассмотренных возможных вариантов ясно, что возможны многие другие приложения и термины "покупатель" и "продавец" используются как удобные обозначения, но не ограничивают эти сущности. В действительности, от "покупателя 110" не требуется

покупать что-либо, а от "продавца 120" не требуется продавать. Аналогично, "интерактивная коммерческая транзакция" не ограничивается транзакциями купли-продажи. Скорее интерактивной коммерческой транзакцией может быть любая транзакция, в которой покупатель 110 предпочитает использовать средство платежа как часть транзакции, или, более обобщенно, любая транзакция, для которой должна быть использована аутентификация покупателя 110. В качестве возможного варианта приложения, не использующего средство платежа, "покупателем" 110 может быть некоторое лицо, "продавцом" 120 может быть страховая компания, полис которой имеет покупатель, и "транзакцией" может быть то, что покупатель предпочитает изменить лицо, получающее пособие. Продавец предпочитает сначала аутентифицировать покупателя, до получения покупателем доступа к своей учетной записи.

На фиг.2 изображена запись событий, иллюстрирующая функционирование 200 системы 100. Способ 200 может быть приближенно разделен на три основных части: регистрация 202 покупателя, аутентификация 204 покупателя и регистрация 206 транзакции. Не во всех реализациях используются все три стадии 202-206, или все индивидуальные этапы, изображенные на фиг.2, но в рассматриваемом возможном варианте они содержатся для иллюстрации различных аспектов изобретения. При регистрации 202 покупателя между покупателем 110 и службой 130 аутентификации устанавливается секретная информация, которая будет использована на стадии 204 для аутентификации покупателя и средства платежа. Регистрация 202 покупателя предпочтительно для каждого средства платежа происходит только один раз. Аутентификация 204 покупателя происходит в режиме реального времени, как часть интерактивной коммерческой транзакции. На этой стадии покупатель 110 демонстрирует службе 130 аутентификации, что имеет доступ к секретной информации. Если демонстрация доступа прошла успешно, то служба 130 аутентификации информирует продавца 120 о том, что покупатель 110 имеет полномочия использовать средство платежа. На стадии 206 регистрации транзакций служба 130 аутентификации создает запись о транзакции, и эта запись впоследствии может использоваться как доказательство проведения конкретной транзакции.

Использование отдельной службы 130 аутентификации имеет много преимуществ. Например, как будет более понятно из последующего описания, большая часть процесса 204 аутентификации покупателя выполняется службой 130 аутентификации. Служба 130 аутентификации определяет, продемонстрировал ли покупатель 110 доступ к секретной информации и, следовательно, имеет полномочия использовать средство платежа. Покупатель 110 принимает участие только в минимальной степени, а продавец 120, по существу, не принимает участия совсем. Сосредоточение этой функции в службе 130 аутентификации приводит к значительной гибкости и снижает расходы на масштабирование. Например, для создания защиты разного уровня для разных средств платежа могут использоваться разные виды секретной информации, от простых персональных идентификационных номеров (ПИН) до сложных протоколов цифровой сертификации. Разные виды секретной информации обычно требуют разной инфраструктуры для выполнения стадии 204 аутентификации покупателя. Сосредоточение стадии 204 аутентификации покупателя в службе 130 аутентификации позволяет распределить стоимость этой инфраструктуры на многих продавцов 120. Дополнительно, если меняется вид секретной информации или соответствующая процедура аутентификации покупателя, то большая часть изменений повлияет только на службу 130 аутентификации, следовательно, позволяя легко реализовать новые технологии аутентификации. Напротив, известные способы, такие как ЗЭТ, требовали от продавца 120 обеспечения большой части необходимой инфраструктуры. Это приводило к большим затратам, медленному внедрению и трудности перехода на новые технологии, что в итоге привело к отказу от ЗЭТ и от подобных подходов.

Этот способ также имеет преимущество, поскольку продавец 120 не получает доступ к секретной информации покупателя 110, так как продавец не принимает участие в аутентификации 204 покупателя. Это предотвращает повторное использование продавцом

120 секретной информации покупателя 110 для санкционирования впоследствии мошеннических транзакций. Например, допустим, что секретной информацией является ПИН. Если бы продавец 120 был ответственен за аутентификацию 204 покупателя, то покупатель 110 должен был раскрыть свой ПИН продавцу 120, который имел возможность использовать его впоследствии в мошеннических целях. Однако в настоящем способе покупатель 110 раскрывает ПИН не продавцу 120, а только службе 310 аутентификации.

Дополнительно, как будет описано ниже, поскольку стадия 204 аутентификации покупателя сосредоточена в службе 130 аутентификации, то может быть осуществлено дополнительное снижение расходов на масштабирование при выполнении службой 130 аутентификации также других функций. Например, служба аутентификации 130 может добавлять к транзакции дополнительную информацию (например, адрес транспортировки для покупателя), обрабатывать или частично обрабатывать средство платежа покупателя и/или создавать и хранить записи транзакций.

Согласно фиг.2 каждый из блоков 110, 120 и 130, выделенных штриховыми линиями, представляет один из компонентов в системе 100. Блоки, выделенные сплошной линией, представляют разные этапы способа 200. Размещение блока, выделенного сплошной линией, внутри блока, выделенного штриховой линией, указывает, что этап, по существу, выполняется этим компонентом. Например, этап 210 размещен внутри блока, выделенного штриховой линией, для службы 130 аутентификации. Это указывает на то, что служба аутентификации 130, по существу, выполняет этап 210. Некоторые этапы имеют два блока, что указывает на то, что этапы выполняются в двух компонентах. Например, один компонент может передавать сообщение другому компоненту. Предпочтительно, этапы реализуются программным обеспечением, выполняющимся на разных компонентах внутри системы 100, возможно, с помощью блоков аппаратного обеспечения. Этапы могут быть реализованы также в аппаратном обеспечении и/или аппаратно-программном обеспечении.

Стадия 202 регистрации покупателя предпочтительно осуществляется перед фактической интерактивной коммерческой транзакцией. На этой стадии 202 между покупателем 110 и службой 130 аутентификации 130 устанавливается секретная информация. Информация является секретной в том смысле, что в идеале она известна и/или доступна только покупателю (или покупателю 110 и службе 130 аутентификации, в случае секретной информации, совместно используемой покупателем и службой аутентификации). Она не является, по существу, доступной общественности или продавцам 120. Дополнительно секретная информация соответствует конкретному средству(ам) платежа, и доказательство доступа к секретной информации будет принято за подтверждение полномочий на использование средства платежа.

Могут использоваться разные виды секретной информации, в зависимости от вида требуемой защиты. Возможные варианты секретной информации включают ПИН или пароль, удостоверение личности, которое хранится в сети (например, для поддержки роуминга), цифровую подпись, используемую при роуминге, программное обеспечение, удостоверяющее личность, например секретный ключ, локальный для машины покупателя, аппаратное обеспечение, удостоверяющее личность, такое как маркер оборудования, или секретный ключ, содержащийся на интеллектуальной карточке, биометрические данные, удостоверяющие личность, и информацию, используемую в криптографических протоколах типа запрос-ответ.

В конкретном возможном варианте, иллюстрируемом фиг.2, секретная информация устанавливается следующим образом. Служба 130 аутентификации принимает (210) информацию подтверждения, которая впоследствии обеспечивает службе аутентификации возможность определить, имеет ли покупатель 110 доступ к секретной информации. Затем служба 130 аутентификации хранит (212) информацию подтверждения, соответствующую средству платежа, например, как часть базы 150 данных профилей покупателя. В одном варианте осуществления, следующим за этой моделью, секретной информацией покупателя является секретный ключ, а соответствующей информацией подтверждения является соответствующий открытый ключ.

В других вариантах осуществления регистрация 202 покупателя выполняется другими способами. Например, служба 130 аутентификации может не хранить информацию подтверждения. Вместо этого, информация подтверждения может храниться в другом месте и при необходимости восстанавливается службой 130 аутентификации. В другом варианте вместо того, чтобы хранить информацию подтверждения, которая отличается от секретной информации, служба 130 аутентификации может просто хранить непосредственно секретную информацию (например, при хранении паролей или хеш-паролей). Как другой возможный вариант регистрация 202 покупателя может осуществляться автономно. Например, покупатель 110 может заполнить заявку и передать ее в банк. Банк осуществляет проверку информации, имеющейся в заявке, выпускает для покупателя 110 кредитную карточку и передает информацию учетной записи в службу 130 аутентификации. Служба 130 аутентификации создает интеллектуальную карточку с внедренной секретной информацией, и интеллектуальная карточка посылается покупателю 110, например, через почтовую службу. Следует отметить, что в последнем возможном варианте регистрация 202 покупателя использует преимущество процесса регистрации кредитных карточек. Регистрация покупателя может использовать также преимущества других процессов.

Предпочтительно, секретная информация формируется покупателем 110, чтобы минимизировать раскрытие секретной информации другим сторонам. Однако в других вариантах осуществления она может формироваться и/или совместно использоваться другими сторонами, например службой аутентификации, особенно, когда предполагается, что риск, вносимый этими сторонами, является небольшим.

На стадии 204 аутентификации покупателя покупатель 110 предпочитает использовать средство платежа как часть интерактивной коммерческой транзакции с продавцом 120. Служба 130 аутентификации как часть транзакции определяет в режиме реального времени, имеет ли покупатель 110 на это полномочия. В конкретном возможном варианте, согласно фиг.2, это осуществляется следующим образом. Покупатель 110 предлагает (220) использовать средство платежа. Например, покупатель 110 может предложить заплатить за покупку, используя кредитную карточку.

Продавцу 120 требуется знать, имеет ли покупатель 110 полномочия использовать средство платежа, поэтому он передает (230) в службу 130 аутентификации запрос на подтверждение полномочий покупателя. В зависимости от средства платежа идентификация службы 130 аутентификации может быть не очевидной сразу. Может существовать несколько служб аутентификации. Например, каждая компания, выпускающая кредитные карточки, может обеспечивать собственную службу аутентификации. Одним способом решения этой проблемы является использование каталога 140, определяющего соответствие средств платежа и служб аутентификации. В этом случае продавец 120 осуществляет доступ к каталогу 140 для определения того, какая служба аутентификации подходит для средства платежа, предъявляемого покупателем 110.

Служба 130 аутентификации определяет, имеет ли покупатель 110 доступ к секретной информации, на этапах 240-246. Служба 130 аутентификации передает (240) покупателю 110 «запрос на запрос». Этот "запрос на запрос" запрашивает доказательство того, что покупатель имеет доступ к секретной информации. Например, если секретной информацией является пароль, то в "запросе на запрос" может запрашиваться пароль. Если секретной информацией является секретный ключ, то в "запросе на запрос" может запрашиваться, чтобы покупатель 110 подписал что-либо цифровой подписью, используя секретный ключ. В одном варианте осуществления "запрос на запрос" также содержит описание интерактивной коммерческой транзакции и обеспечивает покупателю возможность отклонить транзакцию, например, если описание не соответствует представлениям покупателя. Также, в "запросе на запрос" вместо этого может запрашиваться согласие покупателя на осуществление транзакции. Если покупатель 110 предпочитает продолжить, то он передает (242) свой "ответ на запрос" обратно, в

службу 130 аутентификации.

Служба 130 аутентификации извлекает (244) сохраненную ранее информацию подтверждения для средства платежа и использует информацию подтверждения и ответ на запрос для определения, имеет ли покупатель 110 доступ к секретной информации. Например, в варианте осуществления с использованием пароля служба 130 аутентификации хеширует пароль из ответа на запрос и сравнивает его с котированным значением, которое хранится в качестве информации подтверждения. В варианте осуществления с использованием секретного ключа служба 130 аутентификации использует открытый ключ, который хранится в качестве информации подтверждения, для определения, было ли подписанное цифровой подписью сообщение в ответе на запрос действительно подписано цифровой подписью с использованием соответствующего секретного ключа.

Затем служба 130 аутентификации передает (250) продавцу 120 ответ на исходный запрос продавца. Ответ содержит информацию о том, имеет ли покупатель 110 полномочия использовать средство платежа. Также он может содержать дополнительную информацию, как описано ниже со ссылками на этапы 260 и 270. Следует отметить, что во время аутентификации покупателя 204 секретная информация продавцу 120 не передается.

Перед тем как перейти к описанию этапов 260 и 270, следует отметить, что этапы 240-250 аутентификации, иллюстрируемые фиг.2, являются только одним вариантом реализации стадии 204 аутентификации покупателя. Другие реализации будут очевидны. Например, служба 130 аутентификации может раньше принять (230) запрос на аутентификацию от покупателя 110, чем от продавца 120. Как другой возможный вариант, служба 130 аутентификации может не использовать запрос 240 и ответ 242 на запрос. Доказательство доступа к секретной информации, например, может быть включено, как часть исходного запроса 230. Дополнительно, как упомянуто на стадии 202 регистрации покупателя, служба 130 аутентификации может использовать способы помимо информации подтверждения (этапы 244 и 246) для определения, имеет ли покупатель доступ к секретной информации.

Согласно фиг.2 в некоторых вариантах осуществления служба 130 аутентификации может внести (260) в транзакцию дополнительную информацию профиля покупателя. Например, продавец 120 может запросить, чтобы к транзакции был добавлен адрес отгрузки для покупателя. Служба 130 аутентификации должна восстановить эту информацию из базы 150 данных и добавить ее к текущей транзакции. Такая дополнительная информация может быть добавлена в разных местах в ходе транзакции и может включать в себя связь с покупателем 110 или продавцом 120. В возможном варианте с использованием адреса отгрузки у покупателя 110 могут запросить подтвердить адрес, и/или продавец 120 может использовать адрес для вычисления расходов на транспорт, которые, в свою очередь, изменят сумму транзакции в долларах.

Аналогично, служба 130 аутентификации может также обрабатывать (270) транзакцию платежа, например, через шлюз 160, через который осуществляется платеж. В одном крайнем случае служба 130 аутентификации может просто уведомлять (250) продавца 120 о том, что покупатель 110 имеет полномочия использовать средство платежа, но продавец 120 выполняет все остальные этапы, требуемые для обработки средства платежа. В другом крайнем случае служба 130 аутентификации может выполнять этапы для обработки транзакции платежа. В промежуточном случае служба 130 аутентификации выполняет некоторые этапы, а покупатель завершает остальные этапы.

Применение информации профилей покупателей (260) и обработка платежей (270) предпочтительны, поскольку служба 130 аутентификации является, собственно, централизованным пунктом для осуществления таких действий. Как в случае действительных этапов 240-246 аутентификации, может быть реализовано снижение расходов на масштабирование за счет службы 130 аутентификации, выполняющей эти функции, вместо их выполнения каждым индивидуальным продавцом 120.

На стадии 206 регистрации транзакций служба 130 аутентификации сохраняет (280) запись транзакции в архиве 170 транзакций. Достоверность записи будет зависеть от конкретного приложения. Как один возможный вариант, служба 130 аутентификации может просто хранить описания открытого текста транзакции. Как другой возможный вариант, более подходящими могут быть записи с временным маркером, подписанные цифровой подписью. Рассматривая возможный вариант с использованием пароля, упомянутый выше, запись, подписанная цифровой подписью, может быть создана при подписании службой аутентификации записи цифровой подписью с использованием собственного секретного ключа. В возможном варианте с использованием секретного ключа непосредственно покупатель 110 создает запись транзакции, подписанную цифровой подписью, используя свой собственный секретный ключ. В каждом из двух последних примеров результатом является устойчивая (к взлому) запись транзакции, подписанная цифровой подписью, которая может использоваться покупателем НО, продавцом 120 или другими сторонами для разрешения спорных вопросов относительно транзакции.

Фиг. 3-7 иллюстрируют предпочтительный вариант осуществления системы 100 и способа 200. В варианте осуществления с использованием Интернета интерактивная коммерческая транзакция осуществляется через систему, основанную на протоколе передачи гипертекста HTTP, конкретно Интернет. Покупатель 110 получает доступ в Интернет, используя стандартный Web-браузер. Продавцом 120 является электронный продавец, использующий электронную витрину Web-сайта (сайта) в Интернете, в данном случае это фиктивный торговый футбольный центр Пита. Электронная витрина работает на стандартном Web сервере. Служба 130 аутентификации также взаимодействует с Интернетом через Web сервер. Покупатель 110 хочет приобрести в торговом футбольном центре Пита кубок Adidas Eqt. Predator Accelerator, используя в качестве средства платежа свою кредитную карточку. Секретной информацией, используемой для защиты транзакции, является секретный ключ, соответствующий средству платежа. Для удобства этот вариант осуществления будет определен как вариант осуществления на базе Интернет, но это не подразумевает, что данный вариант осуществления является единственно возможным для Интернета.

На фиг. 3 изображена запись событий, иллюстрирующая функционирование варианта осуществления на базе Интернет.

Способ 300, как и способ 200, в общем, может быть разбит на три основных части: регистрация 302 покупателя, аутентификация 304 покупателя и регистрация 306 транзакции. Однако этапы, выполняемые для аутентификации 304 покупателя, и этапы, выполняемые для регистрации 306 транзакции, взаимосвязаны друг с другом.

На стадии регистрации 302 покупателя покупатель 110 устанавливает со службой 130 аутентификации свою "учетную запись". В данном случае это означает, что проводится любая автономная проверка (например, прием подтверждения от компании кредитной карточки, что покупатель 110 имеет полномочия использовать кредитную карточку). Дополнительно для учетной записи формируется пара секретный ключ - открытый ключ, и открытый ключ хранится 312 в базе 150 данных службы аутентификации. В предпочтительном варианте осуществления открытый ключ хранится в форме цифрового сертификата, показывающего, что открытый ключ соответствует учетной записи покупателя.

В этом варианте осуществления учетная запись и пара ключей соответствуют нескольким средствам платежа, включая конкретную кредитную карточку, которая будет использована. Другими словами, цифровой сертификат и пара ключей скорее соответствуют "бумажнику" покупателя, который содержит много средств платежа, чем одному конкретному средству платежа. Однако другие варианты осуществления могут использовать другие схемы, например использование разных учетных записей и пар ключей для каждого средства платежа. Дополнительно покупатель 110 может иметь несколько учетных записей и пар ключей. В этом варианте осуществления секретные ключи покупателя и соответствующие службы инфраструктуры открытого ключа (ИОК)

организуются для покупателя 110 агентом программного обеспечения, конкретно Персональным Доверенным Агентом (ПДА) VeriSign. ПДА обеспечивает универсальный ключ и функциональные возможности управления сертификатом и разработан с возможностью простого включения в Web приложения.

ПДА VeriSign управляет удостоверениями личности ИОК покупателя. Например, если покупатель 110 не имеет цифрового сертификата или пары ключей, то ПДА сопровождает покупателя 110 к странице регистрации сертификата. Если цифровой сертификат покупателя скоро истечет, то ПДА предлагает покупателю 110 восстановить сертификат перед продолжением (процесса) и переводит покупателя 110 к странице возобновления сертификата. Также если сертификат покупателя уже истек, то ПДА предлагает вариант перехода на страницу возобновления сертификата для восстановления истекшего сертификата. Все это реализуется посредством диалогов, согласующихся с разными браузерами. Дополнительно, хотя данный конкретный вариант осуществления использует браузеры, ПДА также поддерживает другие устройства, например радиотелефоны и карманные ПДА.

ПДА и секретные ключи могут быть размещены в нескольких местах. В этом возможном варианте на отдельном сервере (не показан) размещено программное обеспечение, реализующее ПДА, и хранятся соответствующие секретные ключи. Одним преимуществом такого подхода является то, что поскольку ПДА и секретные ключи реализуются как нулевой клиент (клиент с нулевым номером), размещенный в службе, то нет необходимости изменять браузер покупателя. Другим преимуществом является то, что, поскольку браузер покупателя не требует никакого специального программного обеспечения, то покупатель 110 потенциально может получить доступ к ПДА и к своим секретным ключам из любого стандартного браузера. Возможный вариант реализации такого доступа описан в находящейся в процессе одновременного рассмотрения патентной заявке США № 09/574.687, "Обеспечиваемое сервером восстановление стойкой секретности из нестойкой секретности", поданной 17 мая 2000 года на имя Warwick Ford. Если ПДА и служба 130 аутентификации размещены на одном сервере, то две функции могут быть до некоторой степени объединены. В другом возможном варианте осуществления ПДА и/или соответствующие секретные ключи реализуются в клиенте покупателя (в программе-клиенте покупателя). Например, ПДА может быть реализован как интегрируемый программный модуль (например, элемент управления ActiveX) в браузере покупателя, а секретные ключи могут храниться локально в программе-клиенте покупателя или в выделенном аппаратном обеспечении (например, устройстве идентификации).

Для рассмотренного выше примера, относящегося к футболу, после регистрации 302 покупатель 110 делает покупки в торговом центре Пита и принимает решение купить некоторые изделия. На фиг. 4 изображен экран браузера покупателя, когда он начинает процесс проверки. Форма заказа 400 в формате гипертекстового языка описания документов (HTML) содержит область 410 заказа, а также кнопку 420 для осуществления срочного аутентифицированного платежа. В области заказа указано, что для этого заказа общая сумма вместе со сбором составляет 59.95$. Покупатель 110 может закончить проверку без аутентификации, используя остальную часть формы, заполняя информацию кредитной карточки, адрес расчета (биллинга) и т.д. Однако покупатель 110 предпочитает использовать аутентифицированный платеж и щелкает кнопку 420 "AuthPay" для осуществления аутентифицированного платежа.

В результате щелчка кнопки 420 аутентифицированного платежа из браузера покупателя передается (330) запрос на аутентификацию в службу 130 аутентификации. Запрос содержит описание транзакции платежа и также идентифицирует продавца 120. Служба 130 аутентификации на этапах 340-346 определяет, имеет ли покупатель 110 доступ к секретной информации (в этом случае секретному ключу для выбранной учетной записи). Более конкретно, служба 130 аутентификации передает (340) покупателю 110 запрос на запрос. В запросе на запрос у покупателя 110 запрашивается подписать некоторые данные цифровой подписью, используя секретный ключ для выбранной учетной записи.

Покупатель 110 передает 342 свой ответ на запрос обратно службе 130 аутентификации. Служба 130 аутентификации извлекает открытый ключ, который был сохранен ранее, и использует его для определения (346), имеет ли покупатель 110 доступ к соответствующему секретному ключу. Процесс аутентификации обычно выполняется между компьютерами, без активного участия реального покупателя 110.

В этом варианте осуществления используется также ПДА для обеспечения покупателю 110 возможности выбрать из своих учетных записей учетную запись, которую он предпочитает использовать, и для выбора затем конкретного средства платежа из средств платежа, соответствующих этой учетной записи. Более конкретно, щелчок кнопки 420 вызывает взаимодействие Web-браузера покупателя с ПДА, осуществляемое посредством диалоговых окон, изображенных на фиг. 5A и 5B. Согласно фиг. 5A покупатель 110 определяет учетную запись, которую он предпочитает использовать, заполняя поле 510 Имя Пользователя и затем вводя правильный пароль 520, аутентифицирует себя для ПДА. ПДА отображает диалоговое окно, которое содержит визуальное представление 530 выбранной учетной записи, согласно фиг. 5B. Покупатель 110 подтверждает, что предпочитает использовать эту учетную запись, щелкая кнопку 540 Вход в систему (Регистрация). Тогда становится доступным секретный ключ, соответствующий учетной записи, для аутентификации и цифровой подписи.

Если покупатель 110 безуспешно выполнил этап аутентификации, то служба 130 аутентификации предпринимает соответствующие действия. Например, служба может уведомить продавца 120, что покупатель не был аутентифицирован. В другом варианте служба может отказаться продолжить обработку транзакции и вернуть покупателя 110 к более раннему экрану (например, экрану 400 проверки).

Если покупатель 110 аутентифицирован, то служба 130 аутентификации вносит (360) в транзакцию дополнительную информацию профиля покупателя. В этом случае служба 130 аутентификации извлекает информацию профиля покупателя и передает эту информацию к браузеру в форме, изображенной на фиг.6. Информация содержит разные средства 610 платежа для этой учетной записи, а также разные адреса 620 отгрузки. Информация профиля покупателя может иметь конфиденциальный характер, поэтому предпочтительно, чтобы служба 130 аутентификации аутентифицировала покупателя 110 перед передачей ему этой информации. В форме также повторяется информация 630, касающаяся транзакции. Покупатель 110 выбирает средство 610 платежа и адрес 620 отгрузки и пересылает форму щелчком кнопки Продолжить.

Покупатель 110 и служба 130 аутентификации создают (380) запись транзакции, подписанную цифровой подписью, используя форму и диалоговое окно, которые изображены на фиг. 7A и фиг. 7B. В ответ на представление формы 600 служба 130 аутентификации возвращает форму, изображенную на фиг. 7A, которая содержит краткое описание 710 транзакции и запрос на санкционирование транзакции покупателем 110. Покупатель 110 санкционирует транзакцию, щелкая кнопку 720 Санкционировать Транзакцию. При этом вызывается диалоговое окно ПДА, которое изображено на фиг. 7B. Щелкая кнопку 730 Подписать, покупатель обеспечивает посредством ПДА подписывание краткого описания транзакции цифровой подписью, создавая при этом запись транзакции, подписанную цифровой подписью. Затем служба 130 аутентификации уведомляет 350 продавца 120 о том, что покупатель имеет полномочия использовать средство платежа и предпочтительно также уведомляет покупателя о том, что транзакция была подтверждена.

В этом варианте осуществления служба 130 аутентификации также осуществляет обработку (370) средства платежа для продавца 120 через шлюз платежа 160, например обслуживание потока платежей Payflow, являющегося доступным для VeriSign.

Передача информации между покупателем 110, продавцом 120 и службой 130 аутентификации, согласно способу 300, выполняется с использованием стандартных Web способов. Например, следует отметить, что форма 400 обслуживается продавцом 120, но щелчок кнопки 420 Аутентифицированного Платежа автоматически передает управление браузером покупателя от продавца 120 к службе 130 аутентификации. Также если процесс

аутентификации завершен, то браузер покупателя возвращается от службы 130 аутентификации к продавцу 120.

Обе эти передачи выполняются с использованием стандартных способов, например способов Принять (Get), Отправить (Post) и/или Переадресовать. Например, пересылка может быть выполнена методом HTTP POST (Отправить), в форме, содержащей данные, которые будут переданы. Это надежно, но иногда приводит к возникновению нежелательных, промежуточных Web страниц. Однако, чтобы устранить необходимость щелкать по промежуточным страницам, может использоваться автоматически инициируемый командный файл (скрипт) программы-клиента. Другой опцией является HTTP переадресация на унифицированный указатель ресурса URL, содержащий данные, которые будут переданы. Эта опция может устранить промежуточные страницы, но в текущее время ограничена в количестве передаваемых данных (поскольку могут быть переадресованы только передачи HTTP Отправить). Другой опцией является HTTP Переадресация на URL, который имеет ссылки на местоположение данных, которые будут переданы, с фактической передачей данных посредством некоторого другого механизма. Этот способ является более сложным, чем другие два способа, но может устранить промежуточные страницы, не ограничивая количество данных, которые могут быть переданы. Данные передаются с помощью некоторого другого механизма, и в адресате им присваивается идентификатор, и они кэшируются. Затем покупатель 110 переадресуется на URL, содержащий назначенный идентификатор.

В качестве упрощенного примера допустим, что при щелчке кнопки 420 аутентифицированного платежа осуществляется передача службе 130 аутентификации запроса на аутентификацию. В одном варианте осуществления это достигается путем использования формы 400, имеющей следующую структуру:

<form method=post action="https://authpay.verisign.com/ authenticate.dll">
<input type="hidden" name="returnURL" value="https://
www.seller.com/process">
<input type="hidden" name="msg" value="PayerAuth Request goes
here">
<input type=submit value="Auth Pay"> </form>.

При этом https://authpay.verisign.corn/authenticate.dll представляет URL службы 130 аутентификации. Поле returnURL определяет местоположение Web-сайта продавца 120, к которому покупатель 110 возвращается после завершения аутентификации. Поле msg содержит запрос на аутентификацию. Для поддержки дополнительных функций могут использоваться другие поля, например, для внесения информации профиля или для обработки платежа.

После завершения процесса санкционирования платежа управление покупателем 110 передается от службы аутентификации 130 обратно продавцу 120 через HTTP Отправить к returnURL, определенному в запросе. HTML форма, которая передается обратно продавцу 120, имеет следующую структуру:

<form method=post action="https://www.seller.com/process"> <input type="hidden" name= "transID" value="123456789"> <input type="hidden" name="msg" value="PayerAuth Response goes here">

<input type=submit value="Continue"> </form>.

Поле transID содержит идентификатор транзакции, который может использоваться покупателем 110 или продавцом 120 для определения транзакции в архиве 170 транзакций. Поле msg содержит ответ продавцу 120 из службы аутентификации 130.

Хотя изобретение подробно описано на примере некоторых предпочтительных вариантов осуществления, возможны другие варианты осуществления. Например, в беспроводных вариантах осуществления (например, основанных на протоколе беспроводных приложений (ПБП) WAP) связь между покупателем 110, продавцом 120 и службой 130 аутентификации, частично или полностью, осуществляется через беспроводные соединения или через шлюзы, соединяющие беспроводную инфраструктуру

с проводной инфраструктурой. Например, покупатель 110 может осуществлять связь с помощью карманного устройства, поддерживающего ПБП. Следовательно, изобретение не ограничивается приведенным здесь описанием предпочтительных вариантов осуществления.

Формула изобретения

1. Способ аутентификации платежной транзакции в сети, содержащий сохранение открытого ключа, ассоциированного с парой ключей инфраструктуры открытого ключа (ИОК), в базе данных профилей, в ответ на прием запроса аутентификации от покупателя по сети, причем запрос аутентификации включает в себя описание платежной транзакции и идентификацию продавца, передачу покупателю по сети «запроса на запрос», причем «запрос на запрос» включает в себя сводку платежной транзакции для отображения покупателю и подписания покупателем цифровой подписью с использованием секретного ключа, ассоциированного с парой ключей ИОК,

в ответ на прием «ответа на запрос» от покупателя по сети, причем «ответ на запрос» включает в себя подписанную цифровой подписью сводку платежной транзакции, определение, имеет ли покупатель доступ к секретному ключу, с использованием открытого ключа для дешифрования подписанной цифровой подписью сводки платежной транзакции, при определении этого, сохранение подписанной цифровой подписью записи платежной транзакции в архиве транзакций и передачу ответа аутентификации продавцу по сети.

2. Способ по п.1, дополнительно содержащий создание пары ключей ИОК и передачу секретного ключа покупателю по сети.

3. Способ по п.1, в котором запись платежной транзакции подписывается цифровой подписью с использованием секретного ключа.

4. Способ по п.1, в котором запись интерактивной транзакции подписывается цифровой подписью с использованием локального секретного ключа.

5. Способ по п.1, в котором открытый ключ сохранен в форме цифрового сертификата, представляющего, что открытый ключ связан с покупателем.

6. Способ по п.1, дополнительно содержащий

извлечение профиля покупателя из базы данных, причем профиль покупателя содержит множество инструментов платежа и множество адресов отгрузки, передачу профиля покупателя по сети покупателю и

прием варианта выбора одного из множества инструментов платежа и одного из множества адресов отгрузки от покупателя по сети.

7. Способ по п.1, дополнительно содержащий обработку платежной транзакции посредством шлюза платежа.

8. Система для аутентификации платежной транзакции по сети, содержащая web-сервер службы аутентификации, связанный с базой данных профилей покупателей, архивом транзакций и сетью, причем web-сервер службы аутентификации адаптивно конфигурирован для сохранения открытого ключа, ассоциированного с парой ключей инфраструктуры открытого ключа (ИОК) транзакции покупателя, в базе данных профилей покупателей, средство покупателя выполнено в виде средства просмотра Web-браузера и предназначено для доступа покупателя в сеть Интернет и запроса аутентификации платежной операции от средства покупателя, включающего в себя описание платежной транзакции покупателя и идентификацию продавца, при этом web-сервер службы аутентификации предназначен для приема по сети запроса аутентификации от средства покупателя, передачи по сети на указанное средство покупателя «запроса на запрос», включающего сводку платежной транзакции для отображения ее покупателю и для подписания покупателем цифровой подписью с использованием секретного ключа, ассоциированного с парой ключей ИОК, сохраняемых в базе данных профилей покупателя, а также приема «ответа на запрос» от средства покупателя, включающего подписанную цифровой подписью сводку платежной транзакции, добавления к данным транзакции

информации профиля покупателя из базы данных профиля покупателей, а также определения, имеет ли покупатель доступ к секретному ключу, с использованием открытого ключа для дешифрования подписанной цифровой подписью сводки платежной транзакции,

причем web-сервер службы аутентификации при определении доступа покупателя предназначен также для регистрации записи платежной транзакции, подписанной цифровой подписью, в архиве транзакций и передачи ответа аутентификации по сети на адрес продавца.

9. Система по п.8, в которой web-сервер службы аутентификации дополнительно предназначен для создания пары ключей ИОК и передачи секретного ключа покупателю по сети.

10. Система по п.8, в которой запись платежной транзакции подписывается цифровой подписью с использованием секретного ключа.

11. Система по п.8, в которой запись интерактивной транзакции подписывается цифровой подписью с использованием локального секретного ключа.

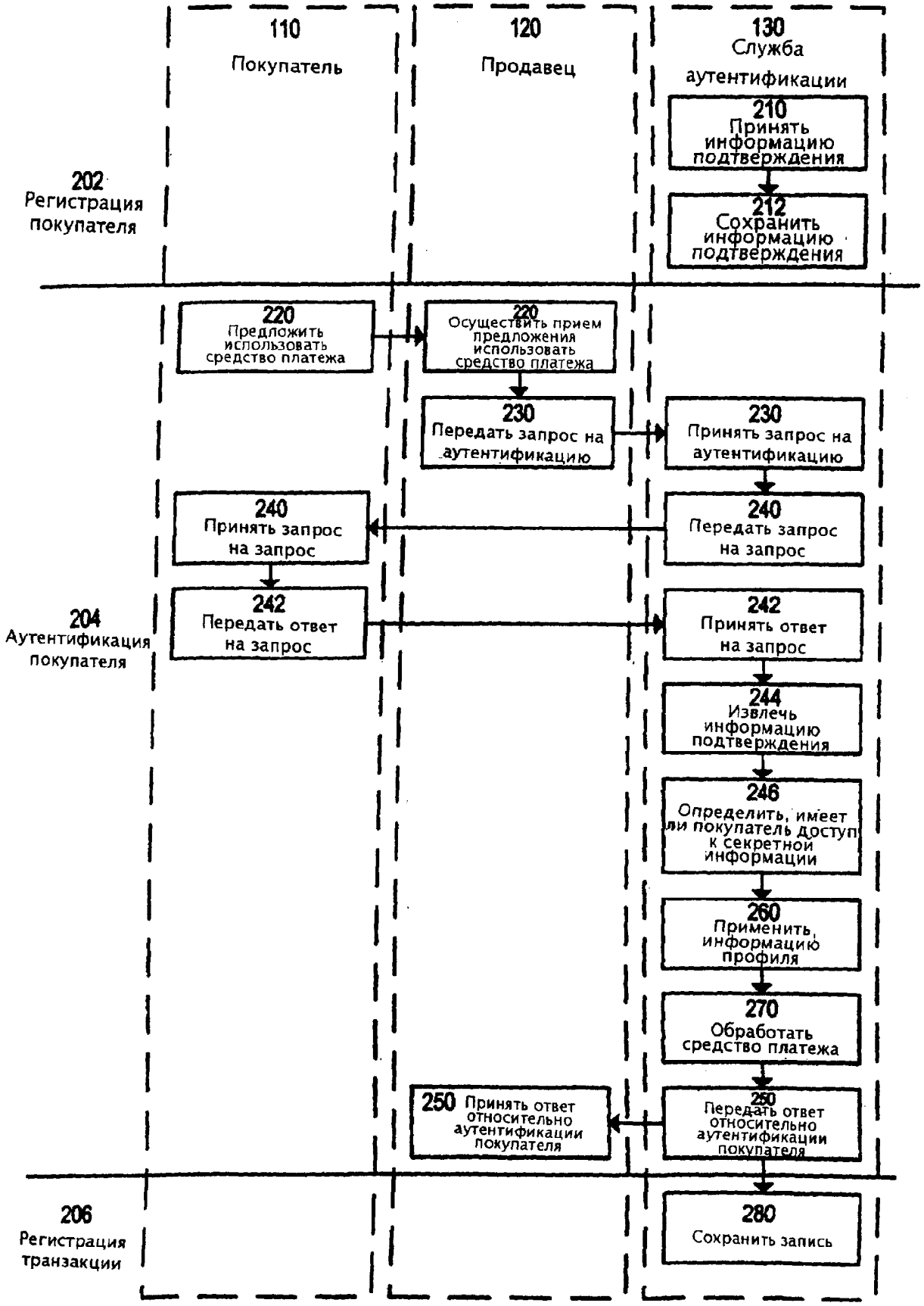
12. Система по п.8, в которой открытый ключ сохранен в форме цифрового сертификата, представляющего, что открытый ключ связан с покупателем.

13. Система по п.8, в которой web-сервер службы аутентификации дополнительно предназначен для

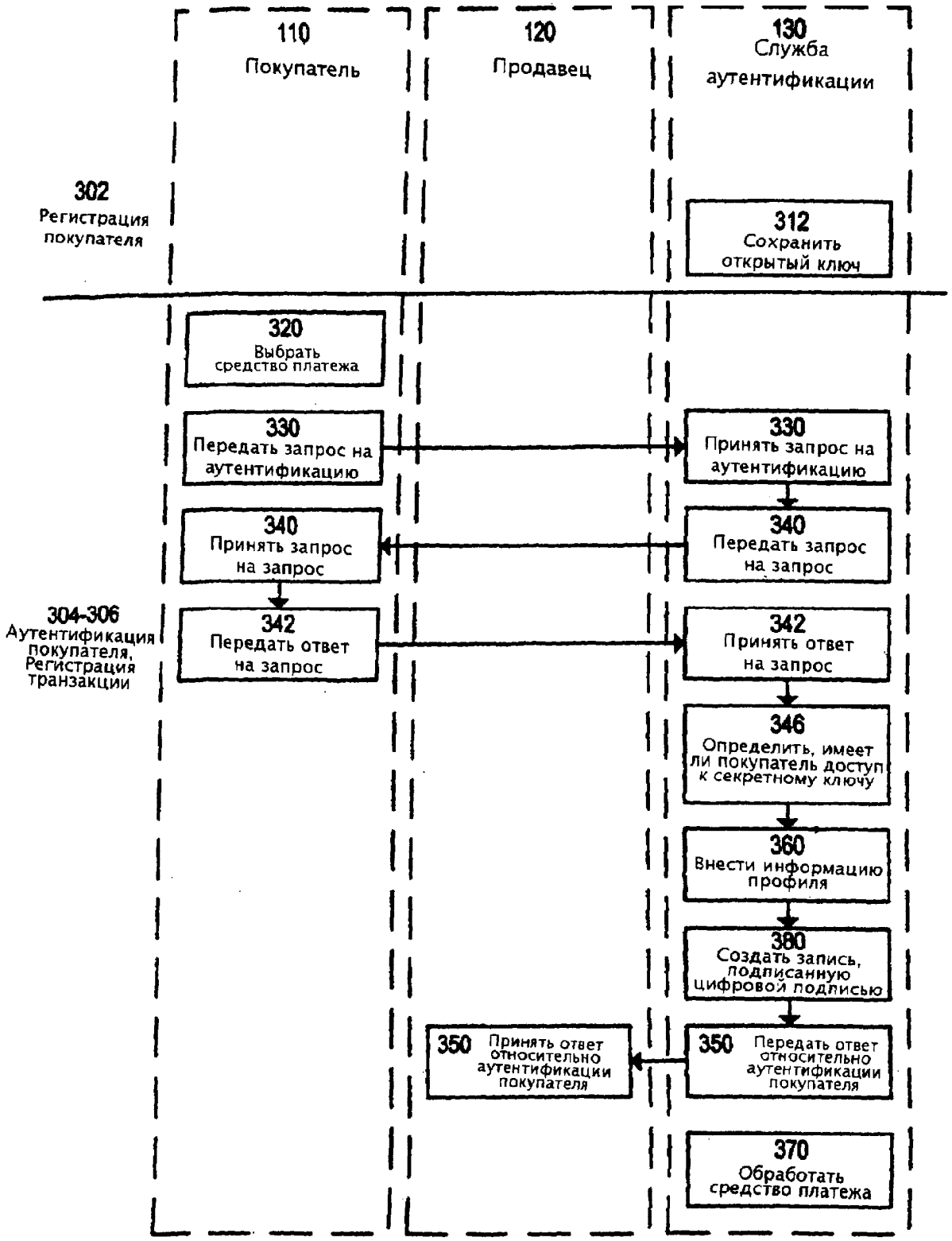
извлечения профиля покупателя из базы данных, причем профиль покупателя содержит множество инструментов платежа и множество адресов отгрузки, передачи профиля покупателя по сети покупателю и

приема варианта выбора одного из множества инструментов платежа и одного из множества адресов отгрузки от покупателя по сети.

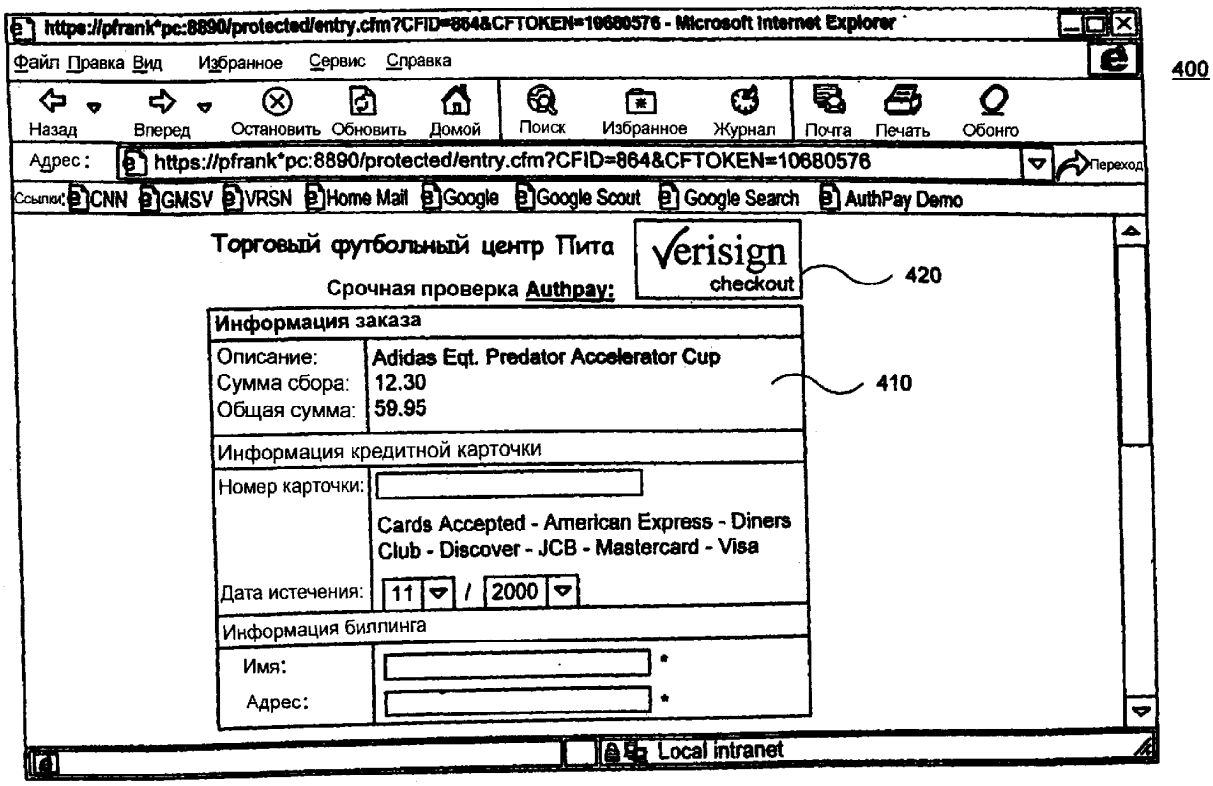
14. Система по п.8, в которой web-сервер службы аутентификации дополнительно предназначен для обработки платежной транзакции посредством шлюза платежа.


110
Покупатель
120
Продавец
130
Служба аутентификации
210
Принять информацию подтверждения
212
Сохранить информацию подтверждения
202
Регистрация покупателя
220
Предложить использовать средство платежа
220
Осуществить прием предложения использовать средство платежа
230
Передать запрос на аутентификацию
230
Принять запрос на аутентификацию
240
Принять запрос на запрос
240
Передать запрос на запрос
242
Передать ответ на запрос
242
Принять ответ на запрос
204
Аутентификация покупателя
244
Извлечь информацию подтверждения
246
Определить, имеет ли покупатель доступ к секретной информации
260
Применить информацию профиля
270
Обработать средство платежа
250
Принять ответ относительно аутентификации покупателя
250
Передать ответ относительно аутентификации покупателя
206
Регистрация транзакции
280
Сохранить запись

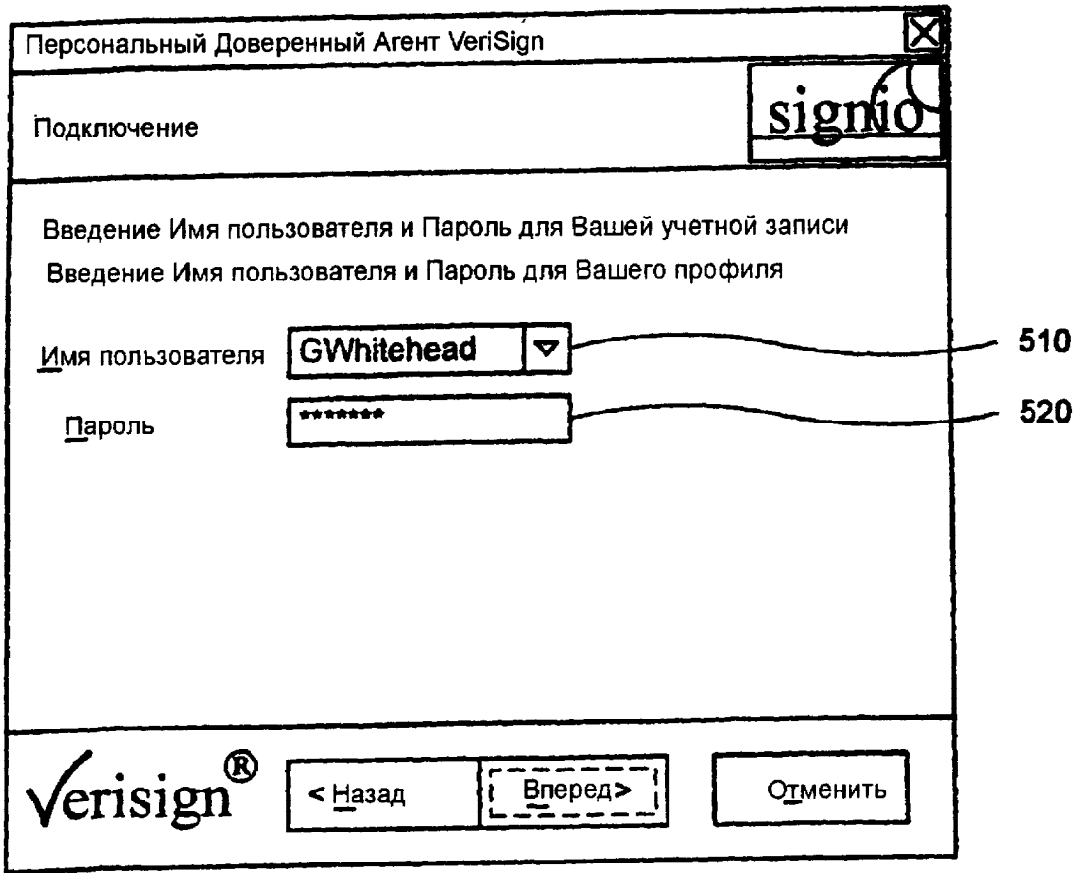
Фиг. 2


110
Покупатель
120
Продавец
130
Служба аутентификации
302
Регистрация покупателя
312
Сохранить открытый ключ
320
Выбрать средство платежа
330
Передать запрос на аутентификацию
330
Принять запрос на аутентификацию
340
Принять запрос на запрос
340
Передать запрос на запрос
304-306
Аутентификация покупателя, Регистрация транзакции
342
Передать ответ на запрос
342
Принять ответ на запрос
346
Определить, имеет ли покупатель доступ к секретному ключу
360
Внести информацию профиля
380
Создать запись, подписанную цифровой подписью
350
Принять ответ относительно аутентификации покупателя
350
Передать ответ относительно аутентификации покупателя
370
Обработать средство платежа

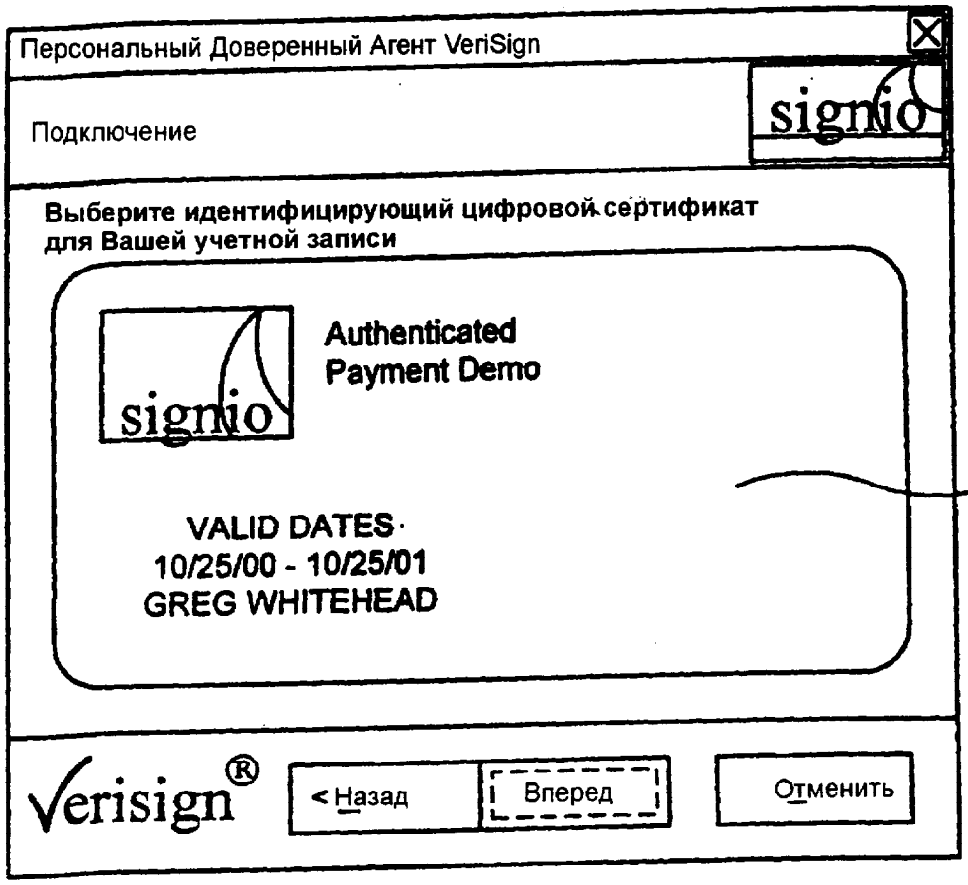
Фиг. 3


https://pfrank*pc:8890/protected/entry.cfm?CFID=864&CFTOKEN=10680576 - Microsoft Internet Explorer
Файл Правка Вид Избранное Сервис Справка
Назад Вперед Остановить Обновить Домой Поиск Избранное Журнал Почта Печать Обонго
Адрес: https://pfrank*pc:8890/protected/entry.cfm?CFID=864&CFTOKEN=10680576
Переход
Ссылки: CNN GMSV VRSN Home Mail Google Google Scout Google Search AuthPay Demo
Торговый футбольный центр Пита
Срочная проверка Authpay:
verisign checkout
Информация заказа
Описание: Adidas Eqt. Predator Accelerator Cup
Сумма сбора: 12.30
Общая сумма: 59.95
Информация кредитной карточки
Номер карточки:
Cards Accepted - American Express - Diners Club - Discover - JCB - Mastercard - Visa
Дата истечения: 11 / 2000
Информация биллинга
Имя:
Адрес:
Local intranet
400
420
410

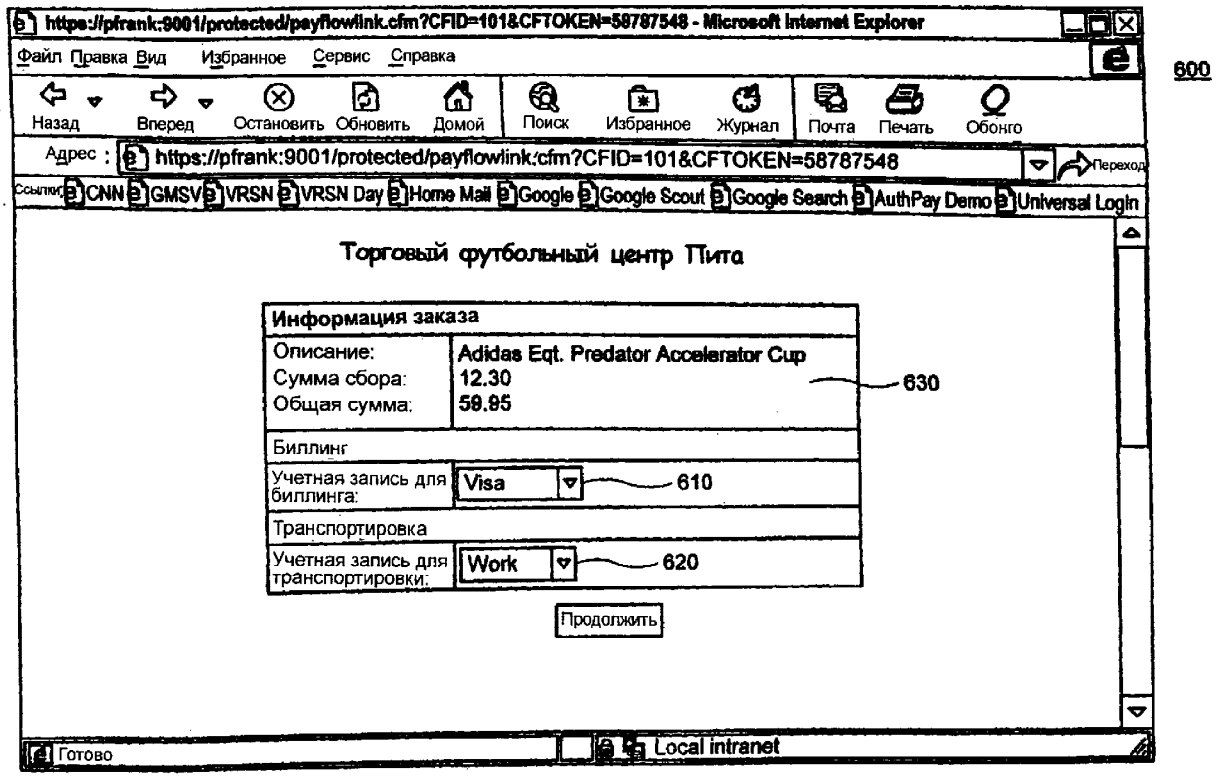
Фиг. 4


Персональный Доверенный Агент VeriSign
Подключение
signio
Введение Имя пользователя и Пароль для Вашей учетной записи
Введение Имя пользователя и Пароль для Вашего профиля
Имя пользователя GWhitehead
Пароль *******
verisign®
< Назад
Вперед >
Отменить
510
520

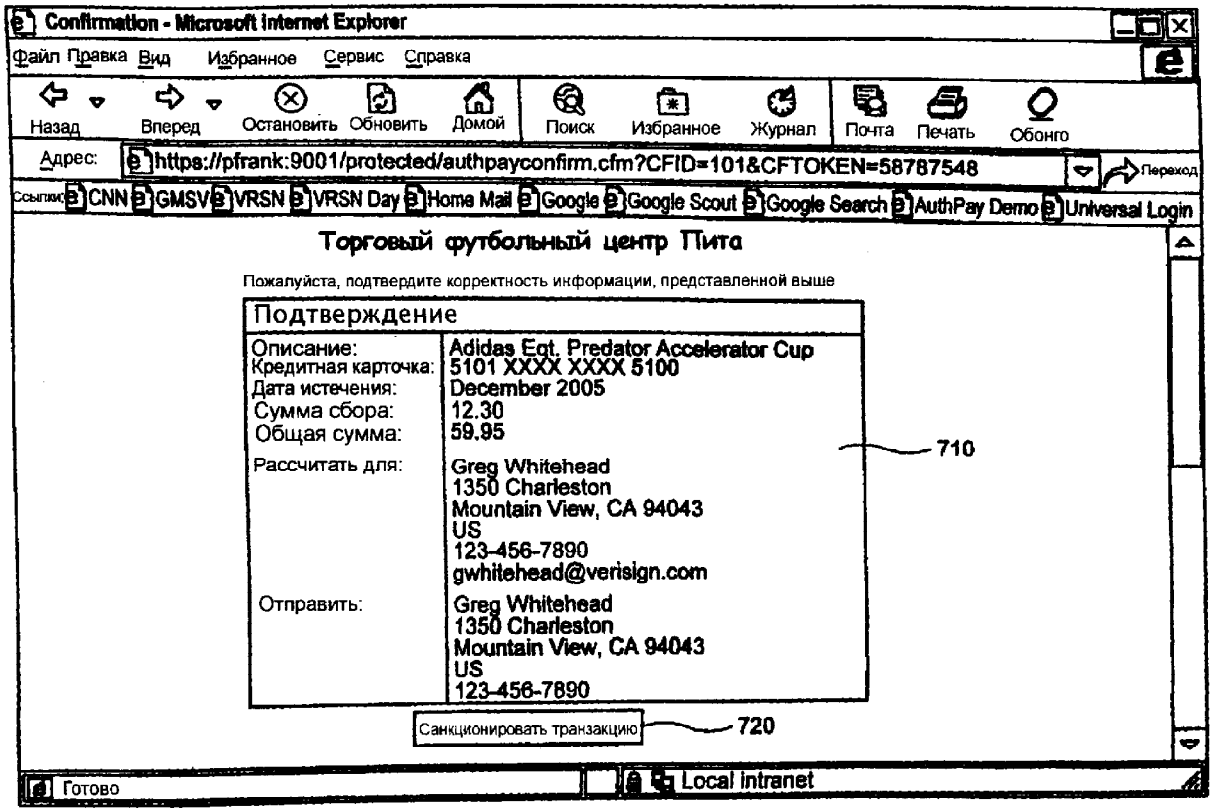
Фиг. 5А


Персональный Доверенный Агент VeriSign
Подключение
signio
Выберите идентифицирующий цифровой сертификат для Вашей учетной записи
signio
Authenticated Payment Demo
530
VALID DATES:
10/25/00 - 10/25/01
GREG WHITEHEAD
Verisign®
< Назад
Вперед
Отменить

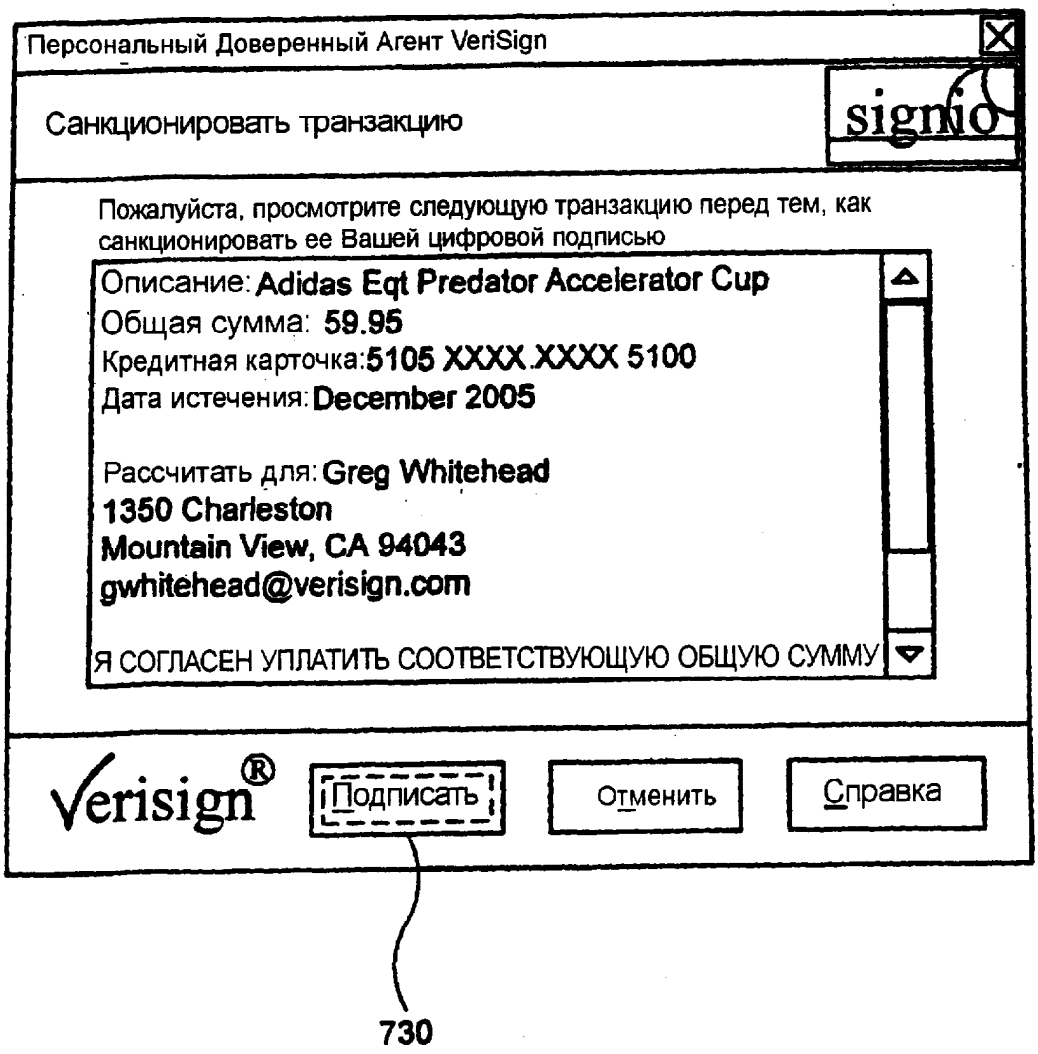
Фиг. 5B


https://pfrank:9001/protected/payflowlink.cfm?CFID=101&CFTOKEN=58787548 - Microsoft Internet Explorer
Файл Правка Вид Избранное Сервис Справка
600
Назад Вперед Остановить Обновить Домой Поиск Избранное Журнал Почта Печать Обонго
Адрес : https://pfrank:9001/protected/payflowlink.cfm?CFID=101&CFTOKEN=58787548
Переход
Ссылки CNN GMSV VRSN VRSN Day Home Mail Google Google Scout Google Search AuthPay Demo Universal Login
Торговый футбольный центр Пита
Информация заказа
Описание: Adidas Eqt. Predator Accelerator Cup
Сумма сбора: 12.30
Общая сумма: 59.85
630
Биллинг
Учетная запись для биллинга: Visa
610
Транспортировка
Учетная запись для транспортировки: Work
620
Продолжить
Готово
Local intranet

Фиг. 6


Confirmation - Microsoft Internet Explorer
Файл Правка Вид Избранное Сервис Справка
Назад Вперед Остановить Обновить Домой Поиск Избранное Журнал Почта Печать Обонго
Адрес: https://pfrank:9001/protected/authpayconfirm.cfm?CFID=101&CFTOKEN=58787548
Переход
Ссылки CNN GMSV VRSN VRSN Day Home Mail Google Google Scout Google Search AuthPay Demo Universal Login
Торговый футбольный центр Пита
Пожалуйста, подтвердите корректность информации, представленной выше
Подтверждение
Описание: Adidas Eqt. Predator Accelerator Cup
Кредитная карточка: 5101 XXXX XXXX 5100
Дата истечения: December 2005
Сумма сбора: 12.30
Общая сумма: 59.95
710
Рассчитать для: Greg Whitehead
1350 Charleston
Mountain View, CA 94043
US
123-456-7890
gwhitehead@verisign.com
Отправить: Greg Whitehead
1350 Charleston
Mountain View, CA 94043
US
123-456-7890
Санкционировать транзакцию
720
Готово
Local intranet

Фиг. 7А


Персональный Доверенный Агент VeriSign
Санкционировать транзакцию
signio
Пожалуйста, просмотрите следующую транзакцию перед тем, как санкционировать ее Вашей цифровой подписью
Описание: Adidas Eqt Predator Accelerator Cup
Общая сумма: 59.95
Кредитная карточка: 5105 XXXX XXXX 5100
Дата истечения: December 2005
Рассчитать для: Greg Whitehead
1350 Charleston
Mountain View, CA 94043
gwhitehead@verisign.com
Я СОГЛАСЕН УПЛАТИТЬ СООТВЕТСТВУЮЩУЮ ОБЩУЮ СУММУ
Verisign®
Подписать
Отменить
Справка
730

Фиг. 7B