



**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ**

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: 2011153984/08, 26.05.2010

(24) Дата начала отсчета срока действия патента:
26.05.2010

Приоритет(ы):

(30) Конвенционный приоритет:
29.05.2009 US 61/182,623;
21.12.2009 US 12/643,972

(43) Дата публикации заявки: 10.07.2013 Бюл. № 19

(45) Опубликовано: 20.07.2014 Бюл. № 20

(56) Список документов, цитированных в отчете о поиске: US 2003115151 A1, 19.06.2003. RU 2 235 359 C2, 27.08.2004. US 6 959 381 B2, 25.10.2005. WO 2007129345 A1, 15.11.2007

(85) Дата начала рассмотрения заявки РСТ на национальной фазе: 29.12.2011

(86) Заявка РСТ:
US 2010/036229 (26.05.2010)

(87) Публикация заявки РСТ:
WO 2010/138611 (02.12.2010)

Адрес для переписки:

129090, Москва, ул. Б. Спасская, 25, строение 3,
ООО "Юридическая фирма Городисский и
Партнеры"

(72) Автор(ы):

**ТАВО Себастьян (US),
НАХАРИ Хади (US),
ДЮПРА Эрик (US)**

(73) Патентообладатель(и):

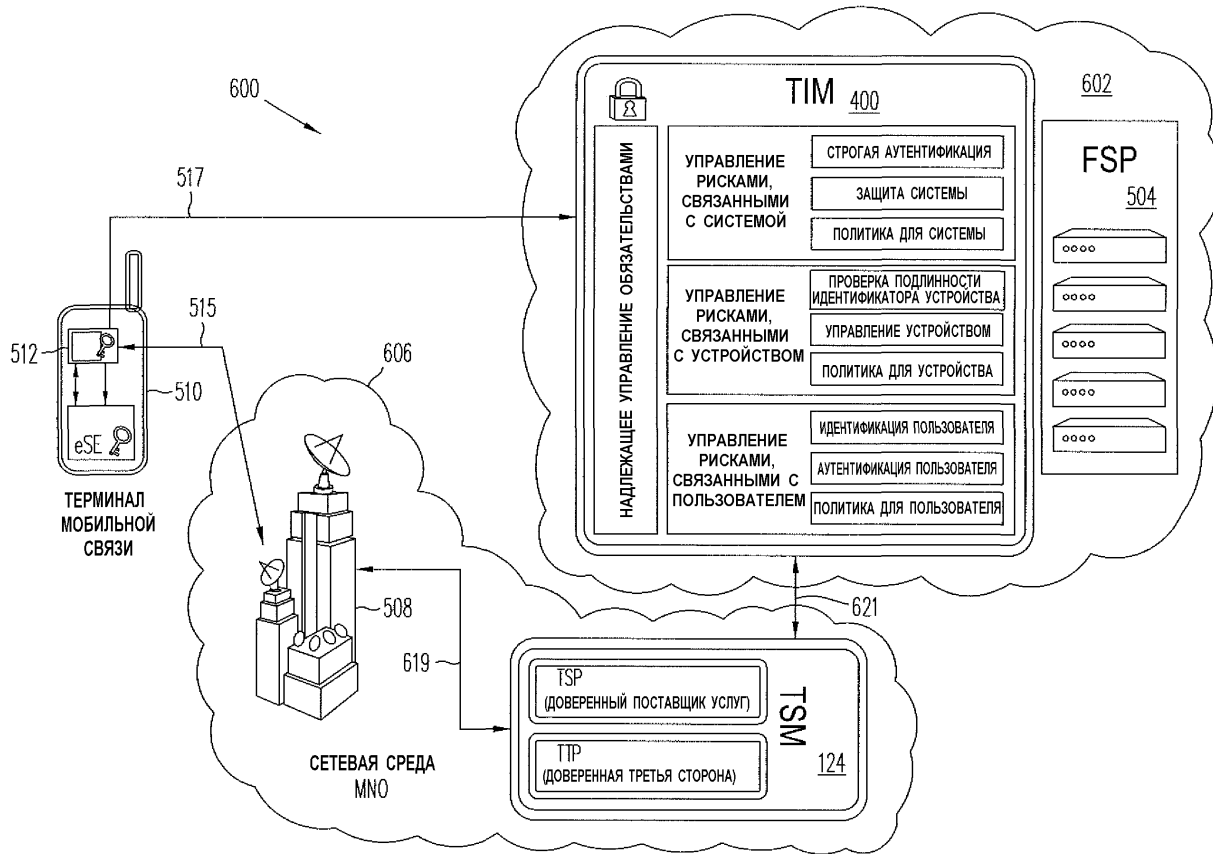
ИБЭЙ, ИНК. (US)

(54) ДОВЕРЕННЫЙ АДМИНИСТРАТОР ДОСТОВЕРНОСТИ (TIM)

(57) Реферат:

Изобретение предназначено для использования в защищенных финансовых транзакциях. Технический результат изобретения заключается в усовершенствованной защите пользователя, защищенности и надежности системы безопасных платежей. Система безопасных платежей включает в себя: сервер, проверяющий подлинность приложения путем сопоставления с уникальными идентификационными данными мобильного устройства и обеспечивающий проверенное на

подлинность приложение для мобильного устройства; и защищенный элемент (SE), действующий в качестве клиента, при этом SE присутствует в мобильном устройстве в качестве клиента. Проверенное на подлинность приложение из сервера устанавливают в SE; и SE исполняет проверенное на подлинность приложение для выполнения процедуры обслуживания, активирующей платежные функции в мобильном устройстве. 3 н. и 17 з.п. ф-лы, 15 ил.



ФИГ.6



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(51) Int. Cl.
G06Q 20/00 (2012.01)

(12) **ABSTRACT OF INVENTION**

(21)(22) Application: 2011153984/08, 26.05.2010

(24) Effective date for property rights:
26.05.2010

Priority:

(30) Convention priority:
29.05.2009 US 61/182,623;
21.12.2009 US 12/643,972

(43) Application published: 10.07.2013 Bull. № 19

(45) Date of publication: 20.07.2014 Bull. № 20

(85) Commencement of national phase: 29.12.2011

(86) PCT application:
US 2010/036229 (26.05.2010)

(87) PCT publication:
WO 2010/138611 (02.12.2010)

Mail address:
129090, Moskva, ul. B. Spasskaja, 25, stroenie 3,
OOO "Juridicheskaja firma Gorodisskij i Partnery"

(72) Inventor(s):
TAVO Sebast'en (US),
NAKhARI Khadi (US),
DJuPRA Ehrik (US)

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

(54) **TRUSTED INTEGRITY MANAGER (TIM)**

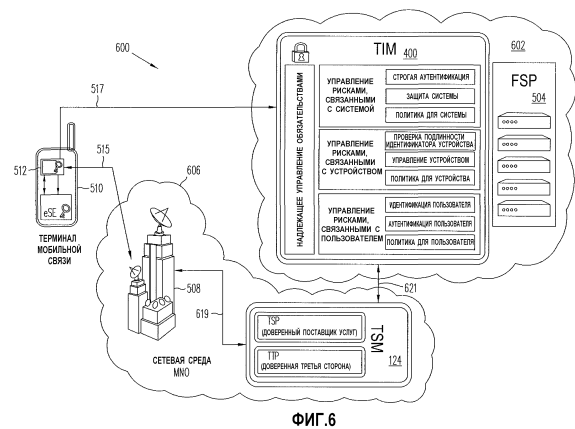
(57) Abstract:

FIELD: physics, computer engineering.

SUBSTANCE: invention is intended for use in secure financial transactions. The secure payment system includes: a server that validates an application by comparing with unique identification data of a mobile device and provides the validated application for the mobile device; and a secure element (SE) acting as a client, wherein the SE is present in the mobile device as client. The validated application from the server is installed in the SE; and the SE executes the validated application to perform a service process, which enables payment functions on the mobile device.

EFFECT: improved user protection, secure and reliable payment system.

20 cl, 15 dwg



C 2
4
3
3
0
4
2
5
2
R U

R U
2
5
2
3
3
0
4
C 2

Перекрестная ссылка на родственные заявки

Для этой заявки испрашивается приоритет на основании предварительной заявки на патент США № 61/182623, поданной 29 мая 2009 г., которая тем самым включена сюда путем ссылки.

5 Предпосылки создания изобретенияОбласть техники, к которой относится изобретение

10 Варианты осуществления настоящего изобретения относятся, в общем, к защищенным финансовым транзакциям, инициированным из электронного устройства, и, в частности, к способности использовать функцию телефона (например, телефонного аппарата мобильной связи) для предоставления данных по каналу обратной связи доверенному администратору достоверности в качестве части программы встроенных мобильных платежей в индустрии финансовых услуг для аутентификации пользователей (например, потребителя).

Предшествующий уровень техники

15 При прямых (личных) или при онлайн-финансовых транзакциях потребители могут искать и покупать товары и/или услуги у торговца. В случае онлайн-покупок транзакции с торговцами интернет-магазинов проводят посредством электронных средств связи через электронные сети. Для проведения таких электронных транзакций могут использоваться различные электронные устройства и различные электронные
20 способы. Способы инициирования или проведения финансовых транзакций из электронного устройства включают в себя, например, SMS (службу передачи коротких сообщений), радиочастотную идентификацию (RFID) или связь ближнего радиуса действия (NFC) в кассовом терминале (POS), и мобильные платежи на основе сети Интернет, посредством которых потребители ищут и покупают товары и услуги у
25 торговцев интернет-магазинов посредством электронных средств связи через электронные сети, такие как, например, сеть Интернет. Такие электронные транзакции могут производиться посредством беспроводной связи, также именуемой связью "по воздуху" (OTA), которая может включать в себя обычную радиосвязь (например, на более длинные расстояния); связь средней дальности, например, связь стандарта Wi-Fi или Bluetooth; или связь ближнего радиуса действия, RFID или NFC (для связи на
30 расстоянии, которое обычно является меньшим, чем приблизительно 4 дюйма (10 см)). Такие транзакции могут быть произведены, например, посредством сотового телефона, в котором используют обычную для сотового телефона радиосвязь, или используют NFC, если сотовый телефон способен поддерживать NFC. Другими мобильными
35 устройствами, помимо сотовых телефонов, которые могут обеспечивать беспроводную связь (OTA) для облегчения таких транзакций, могут являться, в том числе, например, кредитные и дебетовые карты, способные поддерживать радиосвязь, брелки для ключей, мобильные устройства с доступом к сети Интернет, бытовые электронные устройства (одним из которых, в качестве примера, является персональный компьютер или
40 портативный компьютер, снабженный средствами бесконтактной связи и связи ближнего радиуса действия, но этот пример не является ограничивающим) и персональные цифровые информационные устройства (PDA), снабженные средствами бесконтактной связи и связи ближнего радиуса действия.

При регистрации мобильного устройства или при проведении финансовой транзакции
45 проблемой обычно является обеспечение защиты, поскольку данные, передаваемые способом беспроводной связи, обычно могут включать в себя информацию о кредитной карте и о финансовом инструменте, например, имя пользователя, номер счета, персональный идентификационный номер (PIN) и пароль, которая подвергается краже

или атаке злоумышленников. Кроме того, в транзакцию могут быть вовлечены несколько сторон, в том числе, например, потребитель или пользователь, торговец, оператор сети мобильной связи (MNO), поставщик услуг (SP), доверенный администратор обслуживания (TSM), производитель мобильного телефона, 5 производитель интегральной микросхемы (IC) и разработчики приложений (программного обеспечения). Другой основной проблемой, связанной со средствами связи ближнего радиуса действия (NFC) мобильного устройства, является необходимость взаимодействия между многими вовлеченными сторонами помимо финансовых учреждений для удовлетворения запросов потребителя посредством защищенной линии радиосвязи. 10

Краткое изложение сущности изобретения

Согласно одному или большему количеству вариантов осуществления настоящего изобретения, система встроенных мобильных платежей (MEP), управляемая, например, поставщиком финансовых услуг (FSP) в финансовой отрасли, включает в себя 15 доверенного администратора достоверности (TIM), который также может именоваться доверенным поставщиком услуг аутентификации (TAP), который представляет собой часть доверенного администратора обслуживания (TSM) или функционирует совместно с ним. TIM обеспечивает способность использования функции телефонной связи мобильного карманного устройства для предоставления данных (в том числе, например, 20 о времени и о географическом местоположении) в TIM по каналу обратной связи для аутентификации пользователей применительно, например, к финансовым транзакциям. TIM работает совместно с TSM, который может быть описан в широком смысле как примитивная система управления распределением ключей. TIM обеспечивает дополнительную защиту, в особенности, для областей применения, связанных с 25 платежами. TIM включает в себя множество различных подсистем, модулей и компонентов в подсистемах. TIM работает совместно с TSM для обеспечения дополнительной защиты при защищенных транзакциях между субъектами (например, мобильным устройством, поставщиком платежных услуг, финансовым учреждением).

В одном из вариантов осуществления изобретения TIM добавлен к TSM, который 30 управляет связанным с финансами взаимодействием между поставщиками услуг связи, потребителями, предприятиями розничной торговли и финансовыми учреждениями. Обычный TSM имеет только следующие компоненты: доверенный поставщик услуг (TSP) и доверенная третья сторона (TTP). Функции TSP включают в себя следующие приложения: выбора и проверки подлинности, административного управления и 35 выражения в денежном эквиваленте. Функции TTP включают в себя выдачу SIM-карты (модуля идентификации абонента), персонализацию OTA и административное управление сроком службы аппаратных средств (например, для программного обеспечения SIM-карты). Функции TIM включают в себя выполнение различных процедур обслуживания, которые могут включать в себя, например, проверку подлинности, предоставление 40 услуг через TTP, авторизацию и повторную выдачу различных порций информации в мобильном устройстве (также именуемым мобильным телефоном, но которое не ограничено только телефонами) потребителя или пользователя. TIM также осуществляет административное управление данными для проверки подлинности транзакции из удаленного пункта и удостоверяется в безопасности манипуляций с ними (TSM сам по 45 себе может быть подобным большому удаленному центральному устройству электронной обработки данных, платежей или неоплат). За счет связывания функции TIM, действующего в качестве сервера в обычной архитектуре "клиент-сервер", с TSM и со встроенным защищенным элементом (eSE), которые действуют в качестве клиента,

варианты реализации различных вариантов осуществления изобретения могут быть основаны, например, на eSE, на защищенной карте памяти или на карте с универсальной интегральной схемой (UICC) в телефоне, добавлена новая степень проверки подлинности и защиты.

5 Вначале ТТР предоставляет ключ (ключи) SIM-карты поставщику услуг связи. Затем поставщик услуг связи активирует обслуживание пользователя, когда пользователь покупает телефонный аппарат и обслуживание. Это представляет собой обычную активацию. Посредством приложения (также именуемого "app") в телефоне, которое
10 может быть куплено и загружено, например, через магазин приложений, такой как, например, App Store™, являющийся товарным знаком фирмы "Эппл, Инк." (Apple, Inc.) - пользователь выдает запрос на активацию платежных функций в его или ее телефоне. Для того, чтобы добиться более высокого уровня защиты, защищенный элемент (SE), обеспечивающий платежи, который встроен в микросхему радиосвязи (или работающий во взаимодействии с микросхемой радиосвязи), служит хранилищем всех особо важных
15 финансовых данных в телефоне. Загруженное приложение должно быть проверено TSM/TSP до его загрузки. Когда приложение загружено посредством радиосвязи (OTA), то ТТР устанавливает (инсталлирует) его в надлежащем SE и в надлежащей области памяти. В дополнение к этому активируют логический ключ для включения SE для платежей и для привязки его к SIM-карте для связывания по параметрам пользователя/
20 IMEI (международному идентификатору мобильного оборудования). Данные для проверки подлинности должны быть посланы обратно в ТИМ для создания профиля. Мобильное устройство фактически становится платежным устройством с более надежными параметрами обеспечения защиты, чем существующие модели. Средство, обеспечивающее платежи, содержится во встроенном SE, в то время как не являющиеся
25 особо важными или надлежащим образом авторизованные приложения находятся в SIM-карте.

Вторым этапом, например, после предоставления SIM-карты и активации платежных функций, на котором подключение SIM-карты ниже именуют "предоставлением SIM-карты", является обеспечение платежного средства. Пользователь выдает запрос на
30 инсталляцию его/ее платежной карты в телефоне, то есть в телефонной трубке или в телефонном устройстве. Поскольку это устройство представляет собой подвижную станцию, то исходный запрос направляют в TSP (который, например, может проходить через "бумажник" конкретного банка). Затем TSP выдает запрос на проверку подлинности, верификацию и санкционирование того, что конкретное средство, на
35 которое был выдан запрос, является законным средством для этого пользователя. Когда разрешение из банка получено TSM, то в ТИМ посылают информацию, которая подлежит проверке подлинности и упаковке в надлежащем формате для телефона и которую должно понимать встроенное средство SE, обеспечивающее платежи, например, клиентское средство встроенных мобильных платежей (MEP).

40 Затем ТИМ передает "пакет", подлежащий установке во встроенный SE, в ТТР, которая будет устанавливать этот "пакет" в телефоне посредством радиосвязи (OTA). ТТР никогда не осведомлена об используемом способе шифрования или об используемых ключах. В средстве, обеспечивающем платежи, например, во встроенном SE, подлинность всех платежных средств должна проверяться посредством программы
45 ТИМ, выполняемой в телефоне, и проверка их подлинности должна осуществляться регулярно путем сопоставления со сведениями, имеющимися в ТИМ. Кроме того, некоторые данные, связанные с пользователем и с телефоном, могут использоваться ТИМ для проверки подлинности идентификатора или параметров разрешения доступа

при транзакциях посредством обычного способа сбора данных, помимо того, что выполняют на предшествующем уровне техники. Она включает в себя передачу данных о времени и о географическом местоположении по каналу обратной связи из устройства в ТИМ для перекрестной привязки идентификатора торговца (решительная
5 невозможность отказа от обязательств), идентификатора пользователя (сильная защита пользователя) и идентификатора устройства (высокая достоверность используемых платежных средств для банков), а также местоположения и времени транзакции, но эти примеры не являются ограничивающими. Географическое местоположение может быть
10 важным для защиты пользователя, для уверенности в том, что привязка пользователя и устройства, известная ТИМ, действительно соответствует устройству приема платежей у торговца (известному местоположению в финансовой сети) и телефону, используемому для платежа (например, один и тот же город, одна и та же страна).

В другом варианте осуществления изобретения мобильное устройство, снабженное средствами связи ближнего радиуса действия (NFC), определяет, имеется ли надлежущая
15 SIM-карта, имеется ли соединение с оператором сети мобильной связи, были ли изменены данные в SE, встроенном в устройство, и имеется ли реальная SIM-карта. На основании этих условий, например, доверенный дистанционный удостоверяющий агент (TRAA) разрешает пользователю особое использование устройства для платежей посредством, например, связи ближнего радиуса действия (NFC). В частности, например, мобильное
20 устройство, снабженное средствами связи ближнего радиуса действия (NFC), может иметь программное обеспечение TRAA, работающее во встроенном SE в этом устройстве. Встроенный SE производит обмен информацией с SIM-картой устройства. При работе программное обеспечение TRAA проверяет, были ли изменены данные в защищенном элементе. Если они были изменены, и если не поступило подтверждение
25 от TSM или ТИМ через сеть мобильной связи, то устройство является заблокированным и не может использоваться до тех пор, пока не будет дано подтверждение изменения, например, посредством TSM или телефонного звонка поставщику финансовых услуг (FSP). TRAA также проверяет, является ли имеющаяся SIM-карта той SIM-картой, которая фактически используется для обеспечения работы телефона (предоставленной
30 SIM-картой), например, по совпадению уникального идентификатора SIM-карты с ожидаемым. Если SIM-карта не является предоставленной SIM-картой или если SIM-карта отсутствует, то устройство переводят в режим приостановки до тех пор, пока не будет иметься в наличии предоставленная SIM-карта. TRAA также проверяет наличие соединения с сетью и с TSM. Такая ситуация может возникать, например, тогда, когда
35 устройство находится в иностранном государстве, под землей или в тоннеле. Если предоставленная SIM-карта отсутствует, то накладывают заданное ограничение на максимальную сумму транзакции, равную например, 50\$ (долларам США), и транзакции на сумму свыше заданной максимальной суммы (или общей суммы) транзакции не допускаются до тех пор, пока сеть не станет снова доступной для связи с TSM. Этот
40 обусловленный отказ уменьшает риск мошеннических покупок.

Краткое описание чертежей

На чертеже фиг.1 изображена схема системы, на которой проиллюстрирована экономическая система для финансовых транзакций с использованием функции мобильного телефона согласно варианту осуществления настоящего изобретения.

45 На чертеже фиг.2 изображена схема системы, на которой проиллюстрирована часть экономической системы из чертежа фиг.1, относящаяся к доверенному администратору обслуживания (TSM), согласно варианту осуществления настоящего изобретения.

На чертеже фиг.3 изображена блок-схема системы, на которой проиллюстрированы

компоненты TSM согласно варианту осуществления настоящего изобретения.

На чертеже фиг.4А изображена функциональная блок-схема, на которой проиллюстрирован пример функций доверенного администратора достоверности (TIM) на системном уровне согласно варианту осуществления настоящего изобретения.

5 На чертеже фиг.4В изображена блок-схема системы, на которой проиллюстрирован пример подсистем и организации TIM согласно варианту осуществления настоящего изобретения.

10 На чертеже фиг.5 изображена схема системы, на которой проиллюстрирован первый пример мест расположения TSM и TIM в экономической системе для финансовых транзакций согласно варианту осуществления настоящего изобретения.

На чертеже фиг.6 изображена схема системы, на которой проиллюстрирован второй пример мест расположения TSM и TIM в экономической системе для финансовых транзакций согласно варианту осуществления настоящего изобретения.

15 На чертеже фиг.7 изображена схема системы, на которой проиллюстрирован третий пример мест расположения TSM и TIM в экономической системе для финансовых транзакций согласно варианту осуществления настоящего изобретения.

На чертеже фиг.8 изображена схема системы, на которой проиллюстрированы потоки платежей и приложений в экономической системе для финансовых транзакций согласно одному или большему количеству вариантов осуществления настоящего изобретения.

20 На чертеже фиг.9 изображена схема последовательности операций способа и схема взаимодействий, на которой проиллюстрированы системные взаимодействия для экономической системы для финансовых транзакций с использованием функции мобильного телефона согласно варианту осуществления настоящего изобретения.

25 На чертеже фиг.10 изображена последовательность изображений, выводимых на дисплей интерфейса пользователя, иллюстрирующая пример процедуры платежа "одно прикосновение - одно касание" согласно варианту осуществления настоящего изобретения.

30 На чертеже фиг.11 изображена диаграмма взаимосвязей между объектами, на которой проиллюстрировано защищенное связывание по идентификатору (SIB) согласно варианту осуществления настоящего изобретения.

На чертеже фиг.12 изображена блок-схема системы, на которой проиллюстрирован пример строгой аутентификации с нулевым разглашением, основанной на аппаратных средствах, (HOKSA) согласно одному варианту осуществления изобретения.

35 На чертеже фиг.13 изображена диаграмма взаимосвязей между объектами, на которой проиллюстрированы рабочие взаимосвязи доверенного дистанционного удостоверяющего агента (TRAA) на системном уровне согласно варианту осуществления настоящего изобретения.

На чертеже фиг.14 показан пример визуального индикатора интерактивного обнаружения фишинга (IPD) согласно варианту осуществления настоящего изобретения.

40 Подробное описание

Варианты осуществления настоящего изобретения относятся к системам встроенных мобильных платежей (MEP) и к способам обеспечения защищенных финансовых транзакций по сети с использованием доверенного администратора обслуживания. В одном из вариантов осуществления изобретения предусмотрено наличие доверенного администратора достоверности (TIM), который также может именоваться доверенным поставщиком услуг аутентификации (TAP), в дополнение к доверенному администратору обслуживания (TSM), который осуществляет административное управление обменом информацией, связанной с финансами, между поставщиками услуг связи, потребителями,

предприятиями розничной торговли и финансовыми учреждениями. TIM (действующий, например, в качестве сервера системы МЕР и обеспечивающий различные процедуры обслуживания) и способность использования функции телефона (действующего, например, в качестве клиента МЕР) для передачи данных по каналу обратной связи в TIM являются новыми концепциями в финансовой отрасли. За счет связывания серверных функций TIM со встроенным защищенным элементом (eSE) в телефоне, являющемся клиентским устройством, может быть введен новый уровень верификации и защиты в финансовой отрасли.

Функционирование TIM можно считать "доверительной основой" TSM, и оно позволяет поставщику финансовых услуг (FSP), такому как, например, фирма "PayPal, Inc.", не только предоставлять услуги обеспечения, но также и управлять службой аутентификации. TIM обеспечивает основные части, например, "дистанционной" связи, задействованной при использовании связи ближнего радиуса действия (NFC) для транзакций, позволяя приложениям быть заслуживающими доверия и устраняя ответственность, связанную с выполнением заслуживающего доверия приложения в телефонах пользователей, посредством прочной привязки пользователя, счета и платежного средства, документа, имеющего ценность в стоимостном выражении, например, купона или квитанции, и устройства к центральному доверенному и ответственному внутреннему объекту. Другая функция TIM является аналогичной функции центра распределения ключей (КМА) или управляющего центра (СА).

Система МЕР может включать в себя внутреннюю инфраструктуру (бэкенд) и различные рабочие службы. Например, одна рабочая служба может включать в себя аутентификацию отпечатка пальца, данные о котором имеются непосредственно в банковской карте, с использованием цифрового изображения отпечатка пальца, хранящегося или обрабатываемого в хранилище eSE в FSP. Хранилище eSE может находиться, например, в мобильном телефоне пользователя. Может использоваться особый криптографический протокол аутентификации для того, чтобы удостовериться, что "оперативное считывание" отпечатка пальца (например, обработка данных в реальном масштабе времени) должным образом совпадает с помеченным изображением, хранящимся в микросхеме, например, в интегральной микросхеме, используемой для реализации eSE. Обработка включает в себя двойную проверку совпадения в реальном масштабе времени, что является элементом новизны по сравнению со способом, которым обычно выполняют аутентификацию отпечатка пальца, данные о котором хранятся в микросхеме.

К тому же, например, другая рабочая служба может содержать службу аутентификации, которая включает в себя возможность целесообразного использования информации о географическом местоположении из телефона, строгой аутентификации отпечатка пальца, маркировки устройства, отметки времени и данных иных типов, которые можно рассматривать как исходные данные. Некоторые из данных этих типов могут быть предоставлены, например, поставщиком услуг связи (например, оператором сети мобильной связи). Пакет исходных данных может использоваться для обеспечения дополнительного средства оценки степени риска для банков-эмитентов в дополнение к обычным данным о транзакции, полученным банками-эмитентами через сеть сбора данных. На основании этого пакета данных FSP может управлять допустимым уровнем рисков и точно регулировать риски, связанные с использованием мобильного телефона, снабженного средствами связи ближнего радиуса действия (NFC).

Например, если телефон находится в автономном режиме, то FSP может реализовать в eSE параметр, ограничивающий ежедневные расходы заданной суммой, выраженной

в долларах, перед тем, как потребовать принудительного (например, обязательного или необходимого как условие для дальнейших расходов) доступа к сети. Этот параметр также может обеспечивать возможность наличия сброса счетчика в eSE в соответствии с требованиями EMV (EMV представляет собой стандарт взаимодействия карт с интегральными микросхемами, где буквы EMV взяты из наименования платежных систем 5 Europa-Mastercard-Visa). Эта способность работать в автономном режиме может быть задействована путем анализа профиля пользователя, устройства и транзакции. При наличии интеллектуального счетчика, связанного с MEF, клиент может разрешать административное управление различными параметрами для санкционирования или 10 отмены транзакции без возврата в сетевую среду ("облако") FSP (см., например, чертеж фиг.5). Такие параметры могут включать в себя, например, резерв денежной наличности, заданную или заранее оплаченную сумму в долларах на пользовательском мобильном устройстве, связанном с внутренним балансом FSP (но превышать этот баланс не разрешено); количество санкционированных транзакций; или предельную ежедневную 15 сумму в долларах, например, 100\$ в день с требованием повторного соединения с сетевой средой FSP, когда эта сумма приближается к предельной, для проверки подлинности и обновления параметров профиля. Интеллектуальный счетчик также может включать в себя способность ведения журнала предыстории транзакций в автономном режиме для обновления сетевой среды FSP при повторном соединении. 20 Возвращаясь к исходным данным, предоставляемым для службы аутентификации, если пользователь желает пропустить аутентификацию отпечатка пальца, то FSP может, например, приписать транзакции более высокую степень риска или потребовать ввод отпечатка пальца для транзакций на сумму свыше определенной пороговой величины, связанной с параметрами. В случае, например, двухточечной (P2P) NFC для 25 классифицированных транзакций служба аутентификации может разрешить FSP посылать по радиосвязи (OTA) заранее верифицированный удостоверяющий документ как для поставщика, так и для покупателя, обеспечивая надежную оплату безналичной транзакции. Одновременно покупатель предоставляет заранее оплаченный, удостоверяющий документ продавцу, информируя продавца о том, что эта оплата была 30 произведена, и покупатель принимает от продавца удостоверяющий документ о том, что оплата действительно была принята, и что товары действительно были отпущены. В этом случае FSP может обеспечивать условное микродепонирование в реальном масштабе времени для обеих сторон.

На чертеже фиг.1 изображена схема системы, на которой проиллюстрирована 35 экономическая система 100 для финансовых транзакций с использованием функции мобильного телефона. На чертеже фиг.1 показан видоизмененный вариант традиционной "модели с 4 углами", способной отражать особенности экономической системы 100, основанной на мобильной связи. На чертеже фиг.1 показана информация и денежные или кредитные потоки 101, 103, 105, 107, 109, 111, которые могут иметь место между 40 различными объектами (например, 102, 104) для поддержки или вследствие финансовой транзакции между потребителем 102 и торговцем 104 в том случае, когда вовлечен эмитент 106 (например, компания по выпуску кредитных карт или банк) и получатель 108 (например, та часть банка, которая получает и выплачивает денежные средства, в противоположность той его части, которая выдает кредиты, то есть эмитенту). Как 45 показано на чертеже фиг.1, потоки 103, 105, 111, 113 между торговцем 104 и получателем 108 могут включать в себя обмен информацией и транзакции, проходящие через сети 110 и банки 112. Аналогичным образом, как видно на чертеже фиг.1, потоки 115, 117, 119, 121 между потребителем 102 и эмитентом 106 могут включать в себя обмен

информацией и транзакции, проходящие через сети 110, банки 112 и финансовые учреждения (FI) 114. Однако, когда обеспечены дополнительные функциональные возможности использования мобильного телефона 116 для облегчения транзакции согласно одному или большему количеству вариантов осуществления настоящего изобретения, то потоки 115, 117, 119, 121 между потребителем 102 и эмитентом 106 могут включать в себя обмен информацией и транзакции, в которые вовлечены дополнительные объекты. Примерами таких дополнительных объектов, как видно на чертеже фиг.1, являются, в том числе, операторы 118 сетей мобильной связи (MNO), производители 120 интегральных микросхем (Chip), производители и поставщики 122 мобильных телефонов (Handset) и доверенные администраторы 124 обслуживания (TSM), что установлено GSMA (Ассоциацией операторов Глобальной системы мобильной связи). Таким образом, существует потребность в координации различных функций обеспечения защиты и доверенного административного управления между вовлеченными субъектами, в том числе, дополнительными субъектами.

На чертеже фиг.2 изображена схема системы, на которой проиллюстрирована часть 200 экономической системы 100 из чертежа фиг.1, относящаяся к доверенному администратору 124 обслуживания. На чертеже фиг.2 проиллюстрировано множество субъектов, с которыми TSM 124 может взаимодействовать и осуществлять связанные с ними виды обслуживания. Как видно на чертеже фиг.2, в экономической системе 100 может иметься множество участников. Для обеспечения защиты и защищенной связи может быть сделано предположение, что ни одна из них не доверяет (или не обязана доверять) другим сторонам. Многие из функций TSM могут быть заданы поставщиками 220 интегральных микросхем (например, поставщиками интегральных схем для телефонов и считывающих устройств) и поставщиками услуг мобильной связи (например, операторами 118 сетей мобильной связи). Виды обслуживания, обеспечиваемые такими функциями, могут являться видами обслуживания низкого уровня в том смысле, что эти виды обслуживания больше связаны с функционированием аппаратных средств, чем с облегчением финансовых транзакций. Таким образом, один или большее количество вариантов осуществления изобретения могут обеспечивать дополнительные функции и виды обслуживания по сравнению с теми, которые обеспечивает TSM 124. Такие виды обслуживания могут относиться, например, к обеспечению защиты, к доверительному административному управлению и к переносу ответственности.

На чертеже фиг.3 изображена блок-схема системы, на которой проиллюстрированы некоторые компоненты TSM, например, TSM 124. Доверенная третья сторона (ТТР) 302 может осуществлять административное управление только физическими аспектами защищенного элемента (SE, см., например, чертежи фиг.4В и фиг.5), такими как, например, центр распределения ключей (КМА), распределение памяти, предварительное или апостериорное обеспечение и каналы радиосвязи (OTA). Таким образом, например, ТТР 302 может обеспечивать центр 304 управления физическим SD (защищенным доменом; защищенной картой памяти, такой как, например, карта типа TrustedFlash) и физическое распределение 306 ключей.

Доверенный поставщик услуг (TSP) 312 может осуществлять административное управление только лишь службами, связанными с SE, такими как, например, проверка подлинности, аутентификация обслуживания и выполнение приложения в или из SE. Например, TSP 312 может обеспечивать услугу аутентификации 314 приложений и портал 316 регистрации услуг.

На чертеже фиг.4А изображена функциональная блок-схема, на которой проиллюстрирован пример функций, которые могут выполняться доверенным

администратором достоверности (TIM) 400 в качестве части системы встроенных мобильных платежей (MEP). TIM 400 может обеспечивать управление 401 обязательствами в дополнение к другим услугам, включающим в себя управление 402 рисками, связанными с системой, управление 403 рисками, связанными с устройством, и управление 404 рисками, связанными с пользователем. Управление 402 рисками, связанными с системой, может включать в себя, например, строгую аутентификацию 4021, защиту 4022 системы и системную политику 4023 (применительно к защите информации, также именуемой InfoSec). Управление 403 рисками, связанными с устройством, может включать в себя, например, проверку 4031 подлинности идентификатора устройства, управление 4032 устройством и политику 4033 для устройства (применительно к InfoSec). Управление 404 рисками, связанными с пользователем, может включать в себя идентификацию 4041 пользователя, аутентификацию 4042 пользователя и политику 4043 для пользователя (применительно к InfoSec).

На чертеже фиг.4В изображена блок-схема системы, на которой проиллюстрирован пример подсистем и организации TIM 400. Как показано на чертеже фиг.4В, TIM 400 может включать в себя несколько модулей 410-490 для выполнения различных функций и способов обслуживания. Способом обслуживания может являться любой способ, который облегчает реализацию обслуживания, и может включать в себя, например, способы, обеспечивающие выполнение функций, описанных со ссылкой на чертеж фиг.4А. TIM 400 может включать в себя, например, следующие модули: модуль 410 управления профилем, модуль 420 обеспечения, модуль 430 консоли, модуль 440 аутентификации, криптографический модуль 450, модуль 460 опроса устройства, модуль 470 управления устройством, модуль 480 связи и соединитель 490.

Модуль 410 управления профилем может включать в себя профили 4101 устройств, в том числе, как видно на чертеже фиг.4В, наборы профилей 4103 для мобильных телефонов, телевизоров, компьютерных приставок к телевизору, бытовых электронных приборов с управлением через компьютерную сеть (NetTop), игровых приставок и других устройств, таких как, например, телевизоры, поддерживающие технологию приема телевизионных трансляций через сеть Интернет (NetTV). Модуль 410 управления профилем также может включать в себя профили 4102 рисков, включающие в себя, как видно на чертеже фиг.4В, группу профилей для пользователей 4104, группу профилей для устройств 4105, и группу профилей для систем 4106. Модуль 420 обеспечения может включать в себя модули 4202 предварительного обеспечения, апостериорного обеспечения, встроенных функций и перемещения. Модуль 430 консоли может включать в себя модули 4302 операций (ops), записи в журнал, текущего контроля, отслеживания. Модуль 440 аутентификации может включать в себя модули 4402 строгой аппаратной аутентификации с нулевым разглашением (H0KSA), аутентификации по характеру поведения, аутентификации по паролю (PWD) и биометрической аутентификации. Криптографический модуль 450 (обозначенный на чертеже фиг.4В как "crypto") может включать в себя модули 4502 набора алгоритмов, забывчивого хеширования (oblivious hashing, OH), верификации и управления распределением ключей. Модуль 460 опроса устройства может включать в себя модули 4602 опроса SIM (модулей идентификации абонента или SIM-карт), eSE (встроенных защищенных элементов), идентификаторов приложений, идентификаторов разработчиков, модуля доверенной платформы TPM/MPM (TPM), модуля доверенной мобильной связи (MTM), модуля GPS (Глобальной системы определения местоположения), идентификаторов платформ и идентификаторов стеков. Модуль 470 управления устройством может включать в себя модули 4702 для

SRUM, SIB (защищенного связывания по идентификатору), TRAA (доверенного дистанционного удостоверяющего агента), стирания/блокировки и делегируемых функций, и модуль 4704 IPD (интерактивного обнаружения фишинга). Модуль 480 связи может включать в себя модули 4802 протоколов сети Интернет (TCP/IP), протокола дальней связи, протокола связи ближнего радиуса действия/связи на основе технологии Bluetooth (NFC/BT) и протокола защищенной передачи SMS (служба передачи коротких сообщений). Модуль 490 соединителя может включать в себя модули 4902 Trinity/IAF (Форум международного аккредитования (International Accreditation Forum, Inc.)), AP (обеспечения аутентификации), рисков и TSM (доверенного администратора обслуживания).

На чертеже фиг.5 изображена схема системы, которая также может быть описана как модель, в центре которой находится банк, на которой проиллюстрирован первый пример мест расположения TSM 124 и TIM 400 в системе 500 встроенных мобильных платежей (MEP) для финансовых транзакций. Как показано на чертеже фиг.5, функции TIM 400 могут быть включены в состав сетевой среды 502 FSP (поставщика финансовых услуг) с функциями, выполняемыми TSM 124. Таким образом, функции обоих администраторов TIM 400 и TSM 124 могут быть обеспечены одним поставщиком услуг, например, FSP 504. На чертеже фиг.5 также показаны другие признаки и элементы, которые могут быть включены в состав системы 500 MEP. Система 500 MEP может включать в себя мобильный телефонный аппарат 510 (показанный на чертеже фиг.5 как "терминал мобильной связи"). Мобильное устройство 510 может включать в себя предоставленную SIM-карту 512 и eSE 514 (встроенный защищенный элемент). Защищенная линия 513 связи внутри мобильных устройств 510 может соединять предоставленную SIM-карту 512 и eSE 514. Мобильное устройство 510 обычно может поддерживать связь по линии 515 связи с внешним миром через сетевые среды 506 MNO. Предоставленная SIM-карта 512 также может поддерживать связь с TIM 400 по линии 517 связи. Оператор 508 сети мобильной связи (MNO) может поддерживать связь с TSM 124 и TIM 400 по линии 519 связи.

На чертеже фиг.6 изображена схема системы, на которой проиллюстрирован второй пример, который также может быть описан как модель с делегируемым или с совместным административным управлением, мест расположения TSM 124 и TIM 400 в системе 600 встроенных мобильных платежей (MEP) для финансовых транзакций. Как показано на чертеже фиг.6, функции TIM 400 могут выполняться поставщиком услуг, например, FSP 504 в сетевой среде 602 FSP, независимо от функций поставщика услуг TSM 124. В примере, показанном на чертеже фиг.6, функции TSM 124 могут выполняться MNO 508 или третьей стороной, функционирующей во взаимодействии с MNO 508 в сетевой среде 606 MNO. Система 600 MEP может включать в себя мобильное устройство 510, поддерживающее связь с MNO 508 по линии 515 связи. MNO 508 может поддерживать связь с TSM 124 по линии 619 связи. TSM 124 может поддерживать связь с TIM 400 по линии 621 связи. Предоставленная SIM-карта 512 мобильного устройства 510 также может поддерживать связь с TIM 400 по линии 517 связи.

На чертеже фиг.7 изображена схема системы, на которой проиллюстрирован третий пример, который также может быть описан как модель, в центре которой находится поставщик услуг связи, мест расположения TSM 124 и TIM 400 в системе 700 встроенных мобильных платежей (MEP) для финансовых транзакций. Как показано на чертеже фиг.7, функции TIM 400 могут быть включены в состав функций, выполняемых TSM 124 и TIM 400, а функции TSM 124 могут быть обеспечены MNO 508 или третьей стороной, работающей во взаимодействии с MNO 508 в сетевой среде 706 MNO,

независимо от поставщика финансовых услуг, например, FSP 504 в сетевой среде 702 FSP.

В примере, показанном на чертеже фиг.7, система 700 МЕР может включать в себя мобильное устройство 510, поддерживающее связь с MNO 508 по линии 515 связи. MNO 508 может поддерживать связь с TSM 124 и TIM 400 по линии 719 связи. TSM 124 и TIM 400 могут поддерживать связь с FSP 504 по линии 721 связи. eSE 514 мобильного устройства 510 также может поддерживать связь с FSP 504 по линии 517 связи.

На чертеже фиг.8 изображена схема системы, на которой проиллюстрированы потоки платежей и приложений в системе 800 МЕР для финансовых транзакций. Чертеж фиг.8 аналогичен чертежу фиг.1, и на нем более подробно показан пример потоков приложений и платежей. Несмотря на то, что на чертеже фиг.8 TIM 400 показан как включенный в состав TSM 124, чертеж фиг.8 применим к конфигурациям, показанным на чертежах фиг.5, фиг.6 и фиг.7.

На чертеже фиг.9 изображена схема последовательности операций способа и схема взаимодействий, на которой проиллюстрированы системные взаимодействия для системы МЕР, такой как, например, система 500, 600, 700 или 800 МЕР, для финансовых транзакций с использованием функции мобильного телефона. На чертеже фиг.9 показаны взаимодействия и потоки между объектами, перечисленными по горизонтали в верхней части диаграммы, которыми являются: пользователи, поставщик услуг связи (например, MNO), TSM/TSP (управление которым может осуществлять FSP), TTP, TIM (управление которым может осуществлять FSP) и банк (например, банк, компания по выпуску кредитных карт или иное финансовое учреждение). Также в верхней части чертежа фиг.9 изображен столбец, обозначенный как "поток", который описывает тип элемента, вовлеченного во взаимодействие между двумя объектами, как последовательность событий, происходящих при перемещении по диаграмме вниз по вертикали.

Группы стрелок на диаграмме иллюстрируют различные события. Так, например, первым событием, проиллюстрированным вверху диаграммы из чертежа фиг.9, может являться предоставление ключей SIM-карты ("ключи SIM-карты", показанные в столбце "поток") из TTP поставщику услуг связи (что обозначено стрелкой 902, идущей от TTP к поставщику услуг связи). После первоначальной покупки телефонов и услуг (вторая запись в столбце "поток") поставщик услуг связи может активировать обслуживание и идентификатор SIM-карты (третья запись в столбце "поток") для пользователя, что обозначено стрелкой 904, идущей от поставщика услуг связи к пользователям.

Следующая группа стрелок (начинающаяся со стрелки 906, идущей от пользователей к TSM/TSP) указывает, что пользователь может выдать в телефон запрос на активацию платежной функции, что может включать в себя, как описано выше, покупку приложения у TSM/TSP (стрелка 906), аутентификацию и проверку подлинности приложения посредством TIM (стрелка 908), упаковку, выполняемую TIM, и предоставление информации о приложении в TTP (стрелка 910) для инсталляции по радиосвязи (OTA) (стрелка 912) в защищенном элементе (SE) телефона, что также описано выше.

Обеспечение телефона, как описано выше, платежным средством (например, кредитной картой, дебетовой картой, заранее оплаченной картой или подарочной картой) также проиллюстрировано в нижней части чертежа фиг.9 посредством набора стрелок, начиная со стрелки 914, отображающей направленный в TSM/TSP запрос пользователя на предоставление услуг. Этот запрос может быть переслан в банк (стрелка 916), который может одобрить финансирование (стрелка 918), например, с банковского счета пользователя. TSM/TSP может послать в TIM уведомление о наличии финансирования для платежного средства (стрелка 920), которое может быть переслано

ТТР (стрелка 922), и ТТР может произвести инсталляцию платежного средства в мобильном устройстве по радиосвязи (ОТА) (стрелка 924).

Взаимодействие с пользователем (также именуемое в FSP как "входной поток") относительно обеспечения может быть описано следующим образом: перед использованием платежного средства в телефоне пользователь загружает (например, из магазина приложений) или запускает заранее установленное приложение FSP из телефона. Запрос на запуск приложения FSP может исходить от пользователя или может быть инициирован поставщиком услуг связи (например, MNO) или банком после регистрации телефона для того, чтобы он стал стать платежным средством. Приложение, также именуемое "клиентским средством встроенных мобильных платежей", может быть установлено в eSE (во встроенном защищенном элементе) и может также именоваться средством FSP, обеспечивающим платежи, хранилищем платежей FSP и приложением FSP.

Когда приложение FSP установлено в eSE, FSP фактически становится управляющим центром и берет в собственность домен-эмитент в eSE в соответствии с технологией, принятой в этой отрасли (включающей в себя, например, спецификации глобальной платформы). Эта функция является одной из функций TIM 400 на заднем плане. Физическая функция ОТА может выполняться партнером ТТР/ОТА. Для ввода в действие механизма ОТА требуется предварительное обеспечение, административное управление которым могут осуществлять поставщики кремниевых интегральных микросхем, или апостериорное обеспечение. Например, имеются известные процедуры, которые уже используются в данной отрасли при производстве или после производства.

Когда приложение установлено, и телефон становится доверенным устройством, и если какие-либо платежные средства не были заранее укомплектованы вместе с приложением FSP, пользователь может выдать запрос на инсталляцию новых или дополнительных платежных средств. Они должны быть инсталлированы в eSE в случае полного использования средства FSP, обеспечивающего платежи. Однако в некоторых случаях банки желают сохранять более значительную степень контроля и могут выдать запрос на то, чтобы в UICC/SIM мобильного устройства (например, мобильного устройства 510) находилось их собственное приложение и средство для еще более выгодного использования средства FSP, обеспечивающее платежи, от другого FSP. В этом случае необходимо, чтобы приложение FSP содержало надлежащий параметр доступа, подлежащий аутентификации, и чтобы было санкционировано его выполнение средством FSP, обеспечивающим платежи.

На чертеже фиг.10 изображена последовательность изображений, выводимых на дисплей интерфейса пользователя, иллюстрирующая пример процедуры платежа "одно прикосновение - одно касание" ("one-touch-one-tap") согласно варианту осуществления настоящего изобретения. Взаимодействие с пользователем применительно к использованию телефона для оплаты может быть описано следующим образом: пользователь запускает приложение FSP "бумажник" или часть приложения FSP (клиентское приложение), не находящуюся в eSE, из интерфейса пользователя или путем связывания приложения FSP с устройством считывания отпечатков пальцев (FP) или регистрации этого приложения в нем. Как показано на выводимых на экран интерфейса изображениях 1001-1005, пользователь плавно перемещает палец пользователя по устройству считывания FP, и платежное средство FSP пользователя, заданное по умолчанию, является активированным. Если не требуется никаких изменений, то пользователь касается своего телефона и продолжает процедуру. На выводимых на экран интерфейса изображениях, которые приведены в качестве примера, на

изображении 1001, выводимом на экран интерфейса, показан индикатор хода выполнения, который является анимированным справа налево и начинает перемещаться вверх, открывая изображение отпечатка пальца пользователя, которым он прикоснулся к устройству считывания FP. На выводимых на экран интерфейса изображениях 1002, 1003, 1004 и 1005 индикатор хода выполнения перемещается в верхнюю часть дисплея, открывая более значительную долю изображения отпечатка пальца по мере перемещения индикатора хода выполнения, и выводимое на экран изображение отпечатка пальца может стать более темным по мере перемещения индикатора хода выполнения при сканировании в верхнюю часть дисплея. Как показано на выводимом на экран интерфейса изображении 1011, индикатор хода выполнения может изменяться на верхний заголовок, показывающий, например, фразу "готов к оплате". На выводимых на экран интерфейса изображениях 1012, 1013, 1014, и 1015 показано анимированное изображение карты, по которой производится финансирование, например, карты, по которой производится финансирование, заданной по умолчанию, которое перемещается в верхнюю часть дисплея, и после того, как изображение карты, по которой производится финансирование, доходит до своего конечного положения, на экране появляются клавиши, например, "отмена" и "изменить". В этот момент пользователю может быть предоставлена, например, возможность изменить источник финансирования, и затем пользователю, возможно, понадобится пройти еще через одно выводимое на экран дисплея изображение (например, еще раз через выводимые на экран интерфейса изображения 1011-1015) для выбора желательного источника финансирования. На выводимых на экран интерфейса изображениях 1021-1025 показаны приведенные в качестве примера изображения для пользователя, которые выводят на экран дисплея после того, как был произведен платеж с использованием мобильного устройства, например, мобильного устройства 510. На выводимом на экран интерфейса изображении 1021 заголовок "готов к оплате" может изменяться на анимированный заголовок "выполняется обработка". На выводимых на экран интерфейса изображениях 1021, 1022 и 1023 изображение карты, по которой производится финансирование, может постепенно исчезать по мере того, как на экране появляется изображение квитанции о покупке. На выводимом на экран интерфейса изображении 1025 после того, как изображение карты, по которой производится финансирование, исчезает с экрана, на дисплее могут появиться подробные сведения о покупке и клавиша "готово", и пользователю может быть предоставлена возможность завершить вывод изображений на экран дисплея. Когда платеж произведен, то FSP может быть способен целесообразно использовать данные из кассового терминала (POS) для фактического извлечения названия магазина, торговой марки и местоположения и для идентификации товара по универсальному товарному коду (UPC) на цифровой квитанции, которую пользователь может пожелать использовать. Дополнительная видимость наименований торговых марок, обеспеченная способом платежа "одно прикосновение - одно нажатие", может являться дополнительной услугой для торговца. В схеме последовательности операций для платежного средства эта видимость создает отличие от обычного взаимодействия с потребителем, при котором в розничном магазине кассовый терминал (POS) отображает только лишь торговые марки сетей (например, Visa®, MasterCard® и другие). Средство FSP, обеспечивающее платежи, может предоставлять преимущество, заключающееся в том, что на мобильном телефоне предусмотрено наличие (например) торговой марки банка, обеспечивающее ее видимость пользователем и создание услуг вокруг этой видимости для торговцев и банков.

На чертеже фиг.11 изображена диаграмма взаимосвязей между субъектами, на

которой проиллюстрирована система 1100 защищенного связывания по идентификатору (SIB), которая может функционировать во взаимодействии с TIM 400. Пример SIB описан со ссылкой на связь ближнего радиуса действия (NFC) в иллюстративных целях; таким образом, в данном контексте NFC использована только лишь в качестве примера

5 уровня связи, и варианты осуществления настоящего изобретения ни являются основанными на технологии NFC, которая использована просто в качестве примера типового канала связи, не зависят от нее. NFC представляет собой технологию двухточечной беспроводной связи (что видно, например, из протокола), которая основана на стандарте ISO 14443 для бесконтактных карт. В NFC используют

10 высокочастотные сигналы ближнего радиуса действия для обеспечения возможности двустороннего взаимодействия между электронными устройствами. Вместе с технологией NFC обычно используют устройство, именуемое "меткой" (также именуемое меткой с радиочастотной идентификацией (RFID-меткой)). Эта метка представляет собой малый физический объект, который может быть прикреплен к изделию или встроен в изделие.

15 RFID-метка содержит внутри себя уникальный цифровой идентификатор (обычно числовое значение). Метки физически прикрепляют к устройству, которое принимает платеж (например, к стиральной машине в прачечной самообслуживания или к торговому автомату). Метки также содержат кремниевые микросхемы, которые позволяют им принимать запросы из устройства, именуемого устройством считывания/

20 записи радиочастотных идентификаторов (RFID), и отвечать на эти запросы. Мобильный телефон, снабженный средствами связи ближнего радиуса действия (NFC), также может являться устройством считывания меток.

Возникающая проблема проверки подлинности идентификатора, в общем, заключается в том, как надежно "связать" метку с устройством. То есть, как

25 гарантировать то, что метка на самом деле идентифицирует физическое устройство, к которому она прикреплена. Существующие в настоящее время способы обычно основаны на физическом связывании, например, путем приклеивания метки к устройству. Мало того, что они могут быть дорогостоящими и создавать проблемы при техническом обслуживании, они также не обеспечивают защиту. Например, злоумышленник может

30 покрыть исходную метку материалом, обеспечивающим электромагнитное экранирование, например, алюминиевой фольгой, а затем прикрепить собственную поддельную метку, имеющуюся у злоумышленника, поверх первоначальной (подменяя, таким образом, устройство) или просто поменять метки на двух устройствах. Результат является одинаковым: предположение о связывании по идентификатору нарушено.

35 Некоторые метки имеют цифровую подпись. В этом случае считывающее устройство может проверять достоверность метки путем проверки цифровой подписи, встроенной в метку (например, путем проверки связывания по идентификатору с использованием инфраструктуры управления открытыми ключами (PKI)). Допущением при такой проверке подлинности является то, что считывающее устройство доверяет стороне,

40 поставившей подпись на данных в метке посредством надежной копии цифрового удостоверения, которое содержит открытый ключ стороны, поставившей подпись. Проверка подлинности связывания по идентификатору метки с подписью не решает проблему связывания по идентификатору. Другими словами, проверка подлинности связывания по идентификатору метки с подписью решает проблему проверки

45 достоверности самой метки, но не защищенного связывания между меткой и устройством. Эту проблему считают основной проблемой управления идентификаторами, и она становится еще более важной, когда во взаимодействия между меткой и устройством вовлечены финансовые транзакции.

Как проиллюстрировано на чертеже фиг.11, при проверке подлинности связывания по идентификатору согласно одному или большему количеству вариантов осуществления изобретения реализовано поддающееся проверке логическое связывание, которое не основано на физическом связывании между меткой 1102 и устройством 1104, которое не поддается проверке. При одноразовой операции идентификатор метки (именуемый "Tag ID") сохраняют в аппаратно защищенном запоминающем устройстве 1106, имеющемся в устройстве, с использованием доверенного компонента программного обеспечения, например, доверенного агента (ТА) 1108. Затем при каждом считывании метки 1102 посредством считывающего устройства 1110, например, мобильного телефона 510, идентификатор метки сверяют с содержимым аппаратно защищенного запоминающего устройства 1106, которое также именуют защищенным хранилищем 1106. Если они совпадают, то идентификатор метки заслуживает доверия и, как предполагают, представляет собой идентификатор устройства 1104.

В одном из вариантов осуществления изобретения требуется наличие в устройстве 1104 следующих компонентов: защищенного хранилища 1106 и ТА (доверенного агента) 1108. Защищенное хранилище 1106 представляет собой защищенное средство хранения информации, в котором хранят сведения о личных идентификационных ключах, например, цифровые личные ключи. Защищенное хранилище 1106 может быть основанным на аппаратных средствах, таких как, например, модуль доверенной платформы (TPM), модуль доверенной мобильной связи (MTM), встроенный защищенный элемент (eSE), или может представлять собой объект с программной защитой, например, защищенный паролем файл, представляющий собой, например, хранилище программных ключей. Защищенные хранилища, основанные на аппаратных средствах, являются предпочтительными, поскольку они потенциально обеспечивают намного более высокий уровень защиты и не чувствительны к исключительно программным атакам (также известным как атаки в масштабе всей системы). Также возможны защищенные хранилища, основанные на программном обеспечении, однако они имеют худшие характеристики с точки зрения защиты.

Доверенный агент или ТА 1108 представляет собой программный объект, который является доверенным и достоверность которого проверяют при каждом использовании ТА 1108. Например, ТА 1108 может являться доверенным дистанционным удостоверяющим агентом (TRAA) согласно варианту осуществления настоящего изобретения и который описан ниже со ссылкой на чертеж фиг.13. Наличие ТА 1108 в считывающем устройстве 1110 (например, в мобильном телефоне 510) является предпочтительным, но не обязательным. То есть, если в считывающем устройстве 1110 существуют другие средства защиты, которые обеспечивают доверие, то проверка подлинности связывания по идентификатору будет столь же эффективной, как и в том случае, когда имеется ТА 1108 в считывающем устройстве 1110. Считывающее устройство 1110 также может иметь защищенное хранилище 1116.

Установление доверия и проверка подлинности могут осуществляться следующим образом:

1) Производитель устройства (или доверенная третья сторона, ТТР) создает ТА 1108 и помещает его в устройство 1104.

2) Вычисляют криптографическую одностороннюю хеш-функцию ТА 1108; ее именуют $H_1(TA)$.

3) Доверенный объект, именуемый "опорой доверия" (Trust Anchor) 1112 (например, в качестве "опоры доверия" 1112 также может действовать FSP 1114 или производитель устройства) ставит цифровую подпись на $H_1(TA)$. Цифровая подпись представляет

собой операцию PKI, которая означает, что "опора доверия" 1112 владеет парой ключей, состоящей из открытого ключа и личного ключа (а именно, соответственно, Key_{public} и $Key_{private}$). "Опора доверия" 1112 ставит цифровую подпись на блок данных $H_1(TA)$, используя его $Key_{private}$. Хеш-функцию TA 1108 с подписью именуют как $S(H_1$
 5 $(TA), Key_{private})$. Запись $S(H_1(TA), Key_{private})$ не означает, что $Key_{private}$ либо появляется, либо является каким-либо образом доступным в этом объекте данных; эта запись является обычной математической записью функции, которая указывает, что для вычислений используют $Key_{private}$. Из этих данных нельзя сделать заключение о значении
 10 $Key_{private}$.

4) Для проверки достоверности $S(H_1(TA), Key_{private})$ необходимо всего лишь иметь доступ к ключу Key_{public} , принадлежащему "опоре доверия" 1112, и полагаться на его достоверность.

5) Процедура проверки подлинности цифровой подписи является программной операцией, которая также может быть очень быстрой. Компонент программного обеспечения, который выполняет проверку подлинности цифровой подписи, именуют V . Компонент " V " программного обеспечения действует следующим образом: $V(S(H_1$
 15 $(TA), Key_{private}), Key_{public})$ и возвращает логическое значение "ИСТИНА" или "ЛОЖЬ" (означающее, соответственно, успешный или неуспешный результат проверки подлинности подписи).

6) Для оптимизации использования памяти защищенного хранилища также вычисляют одностороннюю криптографическую хеш-функцию Key_{public} . Ее именуют $H_2(Key_{public})$.
 20 H_1 и H_2 могут являться одной и той же односторонней криптографической хеш-функцией или могут являться различными односторонними криптографическими хеш-функциями.

7) Key_{public} загружают в основную память устройства 1104 (например, в оперативное запоминающее устройство, или ОЗУ).

8) Например, производитель устройства сохраняет $S(H_1(TA), Key_{private})$, а также H_2
 30 (Key_{public}) и V в доступной только для чтения области памяти устройства 1104, например, в постоянном запоминающем устройстве (ПЗУ). Компонент V также должен находиться в области ПЗУ для исполняемых программ или должно быть помещено в эту область.

9) Теперь достоверность и подлинность TA 1108 могут быть проверены при каждом использовании TA 1108, результат этой проверки подлинности может являться
 35 заслуживающим доверия. Проверку подлинности производят следующим образом:

9.1) Исполняют компонент V в ПЗУ устройства 1104 (если ПЗУ содержит область для исполняемых программ и V находится в ней). Доверие к V является столь же сильным, как и защита ПЗУ (которая является аппаратной защитой, а это означает, что она не чувствительна к исключительно программным атакам).

9.2) Вычисляют $H_2(Key_{public})$ и проверяют его подлинность путем сопоставления с $H_2(Key_{public})$ в защищенном хранилище 1106. Если проверка подлинности является неуспешной, то устройство 1104 считают поддельным. Если проверка подлинности является успешной, то ключ (Key_{public}) (имеющийся в ОЗУ устройства 1104) считают
 45 надежным.

9.3) Вычисляют $V(S(H_1(TA), Key_{private}), (Key_{public}))Key_{public}$. Если компонент V выполнен успешно (то есть, если V возвращает логическое значение "ИСТИНА"), то TA 1108 может заслуживать доверия. В противном случае систему 1100 считают

фальсифицированной.

10) В этот момент, предполагая, что компонент V выполнен успешно, ТА 1108 может заслуживать доверия, и, следовательно, все, кому доверяет ТА 1108, также могут заслуживать доверия. Начиная с этого момента, ТА 1108 осуществляет доступ к идентификатору метки, хранящемуся в защищенном хранилище 1106, и проверяет его, и отвечает на запросы считывающего устройства 1110 на получение идентификатора метки. Поскольку ТА 1108 является доверенным, то ответы ТА 1108 на запросы являются достоверными.

Защищенное связывание по идентификатору согласно одному или большему количеству вариантов осуществления изобретения включает в себя процедуру обеспечения условия "один раз на каждую метку". То есть после того, как метка 1102 прикреплена к устройству 1104, "опора доверия" 1112, используя ТА 1108, считывает идентификатор метки и сохраняет его в защищенном хранилище 1106 устройства 1104. При последующих заменах метки 1102 (например, для технического обслуживания) процедура обеспечения может быть повторена, чтобы идентификатор текущей метки 1102 всегда имелся в защищенном хранилище 1106. Может быть реализовано дополнительное усиление защиты. Например, в инфраструктуре FSP 1114 (например, в TIM 400) могут быть сохранены записи об идентификаторе метки устройства, местоположении устройства по данным Глобальной системы определения местоположения (GPS) и другие данные. К этой инфраструктуре могут обращаться при операциях управления рисками и для других задач обеспечения защиты, аутентификации и идентификации.

После этапа обеспечения всякий раз, когда считывающее устройство 1110 (например, мобильный телефон, снабженный средствами связи ближнего радиуса действия (NFC), который может использоваться для платежей) считывает идентификатор метки, прикрепленной к устройству 1104, считывающее устройство 1110 передает этот идентификатор метки в ТА 1108 устройства 1104. Связь между считывающим устройством 1110 и ТА 1108 устройства 1104 может заслуживать доверия, поскольку обмен информацией происходит между двумя доверенными объектами (например, между считывающим устройством 1110 и ТА 1108 устройства 1104). Прослушивание этого канала связи затруднено (например, при использовании NFC обмен информацией происходит на близком расстоянии), и даже если оно произведено успешно, это не дает в результате какого-либо полезного направления атаки для злоумышленника. Основанием для этого утверждения является то, что злоумышленник должен быть способен успешно: 1) посылать обманный сигнал (то есть поддельный идентификатор Метки) в считывающее устройство 1110 и 2) блокировать ответ, посланный в ТА 1108 устройства 1104.

Возможности удовлетворения двух вышеизложенных условий практически являются ничтожными. Теперь, если идентификатор метки, сообщенный считывающим устройством 1110, не совпадает с идентификатором метки в защищенном хранилище 1106 устройства 1104, то ТА 1108 отвечает сообщением "нет совпадения", которое посылают обратно в считывающее устройство 1110, возможно, но необязательно, записывает это событие в журнал, переводит устройство в состояние "приостановка", поскольку это могло бы указывать факт попытки фальсификации метки или подмены метки. Также в инфраструктуру FSP 1114 может быть послано (устройством 1104, считывающим устройством 1110 или обоими этими устройствами) сообщение "возможная фальсификация метки" для перевода устройства 1104 в состояние "повышенный риск", и это помогает FSP 1114 с его распределенной инфраструктурой

управления рисками (включающей в себя, например, TИM 400).

Если устройство 1104 не включает в себя защищенное хранилище или ТА, то идентификатор метки может быть послан в инфраструктуру FSP 1114 (например, в базу данных TИM 400) во время процедуры обеспечения. В этом случае, всякий раз, когда считывающее устройство 1110 предпринимает попытку транзакции с использованием такого идентификатора метки, сведения о местоположении считывающего устройства 1110 по данным GPS (предполагают, что считывающее устройство 1110 оснащено системой GPS) может быть послано в инфраструктуру FSP 1114, а затем FSP 1114 посылает в считывающее устройство 1110 сообщение с пригодной для использования идентификационной информацией (включающей в себя, например, следующее сообщение: "наши записи показывают, что это торговый автомат, расположенный в доме № 2211 по улице North First St., г.Сан-Хосе, штат Калифорния", или изображение устройства 1104), которая может помочь пользователю считывающего устройства 1110 при определении того, является ли устройство 1104 легальным.

На чертеже фиг.12 изображена блок-схема системы, на которой проиллюстрирован пример системы 1200 строгой аппаратной аутентификации с нулевым разглашением (HOKSA). Одним из основополагающих принципов защиты является строгая аутентификация. Самый строгий тип аутентификации включает в себя комбинацию из более чем одного фактора аутентификации. Одна из таких комбинаций факторов может быть классифицирована следующим образом: 1) то, что Вы знаете, например, пароли, фразы-пароли; 2) то, что у Вас есть, например, аппаратные маркеры, личные ключи; и 3) кем Вы являетесь, например, биометрические данные. Эти артефакты, когда они объединены надлежащим образом, вынуждают злоумышленника подтасовать несколько факторов до того, как он будет способен предпринять серьезную атаку. Несмотря на то, что большинство систем строгой аутентификации являются однофакторными системами, они могут быть объединены с дополнительным фактором, например, с программным или аппаратным маркером, для создания многофакторной системы. Тем, что отличает системы строгой аутентификации от других, более слабых однофакторных способов, является повышенный уровень защиты, в отличие от уровня защиты в однофакторных способах. Даже в способах аутентификации с низкой энтропией ("основанный на догадках") система строгой аутентификации должна обеспечивать защиту от атак без подключения к сети, даже от злоумышленников с полным доступом к каналу связи. Системы строгой аутентификации также обычно обмениваются сеансовым ключом, который позволяет обеспечивать как конфиденциальность данных, так и их достоверность после того, как аутентификация была успешно выполнена.

Заявлено множество систем аутентификации по паролю для решения этой точной задачи, и постоянно предлагаются новые системы аутентификации по паролю. Несмотря на то, что система защиты может быть заявлена путем изобретения системы аутентификации, в которой избегают передачи незашифрованной секретной информации (например, доказательств) в виде простого текста, намного сложнее изобрести систему аутентификации, которая остается защищенной, когда: 1) злоумышленники имеют полные сведения о протоколе; 2) злоумышленники имеют доступ к большому словарю обычно используемых паролей; 3) злоумышленники могут подслушивать всю информацию, передаваемую между клиентом и сервером; 4) злоумышленники могут перехватывать, изменять и фальсифицировать произвольные сообщения, передаваемые между клиентом и сервером; и 5) обоюдно доверенная третья сторона отсутствует.

В системе 1200 HOKSA используют механизм строгой аутентификации, который

основан на "доказательстве с нулевым разглашением" и который усилен путем защиты информации о секретном ключе, основанной на аппаратных средствах, а также необязательными биометрическими технологиями в клиентских системах для инициирования процедуры аутентификации. Система 1200 HOKSA решает задачу защищенной аутентификации в тех случаях, когда "доказывающая сторона" ("prover") (например, сторона, выдавшая запрос на аутентификацию) должна иметь некоторую секретную информацию (например, информацию о личном ключе) и не несет никакой другой секретной информации, и где "проверяющая сторона" ("verifier") (например, получатель запроса на аутентификацию, например, ТМ 400) принимает решение том, следует ли разрешить запрос на аутентификацию или нет. Система HOKSA 1200 удовлетворяет приведенным ниже требованиям: 1) в системе 1200 в клиентских устройствах размещены модули аппаратной защиты для хранения секретной информации; примерами модулей аппаратной защиты являются, в том числе, следующие: TPM (модуль доверенной платформы), MDM (модуль доверенной мобильной связи), SE (защищенный элемент), eSE (встроенный защищенный элемент), карта SD (защищенный домен, защищенная карта памяти, такая как, например, карта типа TrustedFlash); 2) в системе 1200 могут быть использованы биометрические технологии для инициирования процедуры аутентификации; 3) система 1200 не позволяет злоумышленнику выдавать себя за доказывающую сторону даже в том случае, если произведен несанкционированный доступ к каналу связи между доказывающей стороной и проверяющей стороной; 4) система 1200 не требует наличия ТТР (доверенной третьей стороны) во время процедуры аутентификации; и 5) система 1200 потребляет меньше мощности для такого функционирования, чем при обычной аутентификации, основанной на PKI, что делает систему 1200 пригодной также и для портативных устройств с питанием от аккумулятора.

Многие устройства содержат модуль аппаратной защиты какого-либо вида. Сложной задачей является правильное размещение модуля аппаратной защиты и целесообразное использование его возможностей для того, чтобы приложения, требующие защиты, могли бы согласованно и надежно использовать модуль аппаратной защиты. Система 1200 HOKSA выполняет эти задачи за счет хранения информации о личном ключе в защитном устройстве с аппаратной защитой и предоставления доступа к нему только лишь посредством защищенного и аутентифицированного механизма. Этот механизм аутентификации основан на доказательстве с нулевым разглашением.

На чертеже фиг.12 проиллюстрирован один из вариантов осуществления системы 1200 HOKSA и проиллюстрированы ее компоненты. Основными признаками системы 1200 HOKSA являются, в том числе, следующие: 1) установление неразрывной сквозной (E2E) защиты 1202; и 2) обеспечение возможности быстрой, энергоэффективной и строгой аутентификации. Каждый из этих признаков описан ниже. Система 1200, несмотря на то, что она является очень подходящей для бытовых электронных устройств (CED), также применима и для иных сред, чем CED.

Существенным элементом защиты является установление неразрывной цепочки доверия во время обоих из двух этапов, именуемых этапом аутентификации и этапом защиты канала. Когда цепочка доверия ослаблена, разорвана или испорчена, то хакеры имеют возможность использовать слабые места и подвергнуть систему атаке. Например, предположим, что А и В должны выполнить аутентификацию друг друга до установления канала связи, что схематично обозначено следующим образом:

A ← [канал связи] → B

А и В могут именоваться конечными точками канала связи, поскольку в реальных

сценариях канал связи проходит через множество точек соединения, именуемых транзитными участками, что схематично обозначено следующим образом:

$A \leftarrow [(транзитный\ участок_0) \leftrightarrow (транзитный\ участок_1) \leftarrow \dots \rightarrow (транзитный\ участок_n)] \rightarrow B.$

5 Конечные точки могут быть локальными (то есть конечные точки находятся в пределах одного и того же устройства или одной и той же среды выполнения программы), или оконечные точки могут быть чужими (то есть конечные точки принадлежат к различным устройствам или средам выполнения программы). Одним из примеров локальных конечных точек является обычная конструкция вычислительных устройств, таких как, например, персональный компьютер (PC), портативный компьютер 10 или другие СЕД. Примером чужих конечных точек является тот, в котором две (обычно) физически отдельные системы поддерживают связь на расстоянии. В реальных сценариях обычно имеет место гибридный случай, например, комбинация локальных и чужих конечных точек, задействованных в связи и в передаче данных.

15 Важной характеристикой системы HOKSA 1200 является установление сквозного (E2E) доверия 1202, поддающегося проверке, с корнем в модуле 1204 аппаратной защиты (HSM), который именуют "корнем доверия" (ROT) 1206. Цепочку от ROT 1204, 1206 к компоненту, использующему ROT 1206, именуют цепочкой 1202 доверия (COT). Это критически важно, чтобы COT 1202 удовлетворяла двум приведенным ниже условиям 20 на каждом этапе пути от аппаратного ROT 1204, 1206 до компонента, который использует ROT 1206: 1) защита канала; и 2) взаимная аутентификация.

Защита канала означает, что канал связи между двумя конечными точками должен быть защищен на каждом этапе пути, как на приведенной выше второй диаграмме. Понятие "защита канала" также подразумевает, что информационное содержимое 25 канала нельзя легко подслушать. То есть попытки подслушивающие были бы либо очень дорогостоящими, либо очень трудоемкими, либо потребовали бы нетривиального уровня технических знаний, который обычно отсутствует. Защита канала этого типа обычно реализована с использованием аппаратной защиты, криптостойкого шифрования или обоих этих способов.

30 Взаимная аутентификация означает, что на каждом этапе пути, как на приведенной выше второй диаграмме, конечные точки каждого транзитного участка связи выполняют аутентификацию друг друга. Условие взаимной аутентификации может быть ослаблено в том случае, если имеются другие механизмы защиты, или если риски, связанные с ослаблением этого условия, являются пренебрежимо малыми, когда речь идет о сквозной 35 (E2E) защите системы (например, COT 1202).

В этот момент и в силу того, что условия защиты канала и взаимной аутентификации выполнены, требования для первого основного признака системы 1200 HOKSA, заключающиеся в установлении цельной сквозной (E2E) защиты, удовлетворены. Ниже приведено описание того, как удовлетворяются условия для второго основного признака 40 системы 1200 HOKSA, заключающиеся в обеспечении возможности быстрой, энергоэффективной и строгой аутентификации.

HSM 1204 включает в себя аппаратно защищенную область памяти, которую именуют защищенным хранилищем 1208. В данном контексте термин "аппаратная защита" означает, что доступ к содержимому запоминающего устройства могут осуществлять 45 только привилегированные и аутентифицированные объекты, следовательно, обозначается термином защищенное хранилище 1208. В качестве иллюстрационного примера предположим, что некоторая информация ($Key_{private}$) о личном ключе (например, некоторые цифровые данные, которые не должны быть общедоступными)

хранят в защищенном хранилище 1208. ($Key_{private}$) может обладать приведенными ниже качествами: 1) ($Key_{private}$) является уникальным, не может быть подделан или угадан; следовательно, он является идентификатором устройства; 2) ($Key_{private}$) недоступен для неаутентифицированных и несанкционированных объектов, поскольку ($Key_{private}$) хранят в защищенном хранилище 1208; и 3) ($Key_{private}$) может, следовательно, использоваться для строгой аутентификации устройства 1210. Эти три качества удовлетворяют требованию строгой аутентификации из второго основного отличительного признака системы 1200 HOKSA.

Удовлетворение условий по скорости и энергоэффективности для второго основного отличительного признака системы 1200 HOKSA описано следующим образом: ($Key_{private}$) может быть использован в качестве доказательной информации для доказательства сведений с нулевым разглашением. То есть устройство 1210 хранит ($Key_{private}$) в области защищенного хранилища 1208 его 1204 HSM, и затем использует его для участия в доказательстве с нулевым разглашением вместе с внешними объектами, которым необходимо выполнить его аутентификацию. Этот механизм гарантирует то, что ($Key_{private}$) остается конфиденциальным. Варианты реализации доказательства с нулевым разглашением являются намного более быстрыми механизмами по сравнению с другими механизмами (приблизительно на два порядка по величине, например, по сравнению со схемами идентификации на основе RSA (алгоритма Ривеста-Шамира-Адлемана)) и, следовательно, требуют меньшего объема вычислений (например, количества циклов обработки). Это удовлетворяет условию по скорости, которое является необходимым условием для второго основного отличительного признака системы 1200 HOKSA. Имеет место прямая взаимозависимость между количеством циклов обработки и мощностью, потребляемой устройством, выполняющим вычисления, следовательно, удовлетворено условие по энергоэффективности, которое является необходимым условием для второго основного отличительного признака системы 1200 HOKSA.

Доказательство с нулевым разглашением является формальным математическим понятием. Одно из фундаментальных свойств систем формального доказательства этого класса именуют неразличимостью. Любая математическая система доказательства (например, с нулевым разглашением) имеет два класса действующих субъектов: доказывающую сторону (которая доказывает утверждение) и проверяющую сторону (которая проверяет доказательство, предложенное доказывающей стороной). Для определения и оценки безопасности и надежности доказательства, предоставляемого в таких системах, проверяющую сторону считают либо честной проверяющей стороной (то есть проверяющая сторона досконально придерживается протокола системы доказательства), или нечестной проверяющей стороной (то есть проверяющая сторона не придерживается этого протокола досконально). Этот способ позволяет системе проверять правильность заявления вне зависимости от того, придерживается ли проверяющая сторона протокола, предложенного доказывающей стороной. Важным побочным эффектом этого свойства является неразличимость. То есть для доказательства, которое должно подтверждаться (это означает, что какие-либо "сведения" о секрете не разглашают), оно должно быть неразличимым, с точки зрения проверяющей стороны, вне зависимости от честности проверяющей стороны. В более простой формулировке не происходит утечки каких-либо сведений о секрете или о способе, которым доказывают обладание секретом.

На чертеже фиг.13 изображена диаграмма взаимосвязей между субъектами, на

которой проиллюстрированы система 1300 встроенных мобильных платежей (MEP), доверенный дистанционный удостоверяющий агент (TRAA) 1302 и рабочие взаимосвязи на системном уровне. Определение состояния защиты мобильного устройства (например, терминала 1304 мобильной связи), в котором хранятся финансовые инструменты, является не тривиальным. Когда такое устройство (например, терминал 1304 мобильной связи) работает в автономном режиме (то есть, когда становится недоступной связь с собственной сетью 1306 (например, с сетевой средой 1306 MNO), которая является сетью, абонентом которой является это устройство), выполнение этой задачи становится еще более затруднительным, поскольку неприменимы типичные способы дистанционной проверки по импульсам. Для мобильных телефонов (например, для терминала 1304 мобильной связи) одним направлением атаки хакеров для получения привилегированного доступа к терминалу является устранение SIM-карты 1308 (модуля идентификации абонента) или ее отключение иным способом и прерывание канала связи между телефоном 1304, сетью 1306 мобильной связи и другими конечными точками, такими как, например, конечные точки у поставщиков 1310 финансовых услуг (FSP). Атака этого типа облегчает попытку хакеров обойти механизмы сетевой защиты, которые установлены для защиты целостности и конфиденциальности финансовых инструментов в устройстве. Это увеличивает вероятность того, что будет предпринята успешная атака, и, в свою очередь, приводит к возрастанию риска для финансовых учреждений (например, банка 1314, FSP 1310), препятствуя, таким образом, попыткам обеспечения возможности транзакций посредством мобильного телефона 1304 в автономном режиме.

TRAA 1302 решает эти задачи путем обеспечения набора операций проверки по импульсам для гарантии того, что уязвимые соединения (например, соединения 1305, 1309) являются доступными и активными. Если необходимая проверка является неуспешной, то может быть принудительно установлено заданное ограничение. Могут полагать, что защита, обеспечивая TRAA 1302, является настолько же хорошей, как и надежность механизма соблюдения ограничительных правил.

Обеспеченная защита требует наличия 1302 TRAA в мобильном устройстве 1304. TRAA 1302 может представлять собой, например, программное приложение, которое удовлетворяет следующим требованиям:

1) TRAA 1302 сам по себе является заслуживающим доверия. То есть TRAA, 1302 либо хранится в аппаратно защищенном модуле, таком как, например, eSE 1312 (встроенный защищенный элемент) или TPM (модуль доверенной платформы), либо его достоверность может быть проверена и засвидетельствована. Механизмы установления этой проверки достоверности включают в себя способы проверки подлинности цифровой подписи или способы забывчивого хеширования (ОН) (но эти примеры не являются ограничивающим признаком).

2) В TRAA 1302 имеются сведения о той же самой SIM-карте 1308, которая присутствовала тогда, когда мобильный телефон снабжался финансовым инструментом, обеспеченные путем сохранения и защиты значения уникального идентификатора SIM-карты. (См., например, стрелки 902, 904 и стрелки 922-924 на чертеже фиг.9). Эту SIM-карту именуют как предоставленной SIM-картой 1308.

3) TRAA 1302 реализует способ для периодического выполнения следующих операций:

3.1) Операции проверки собственной достоверности: если эта проверка является неуспешной, то финансовые инструменты в телефоне 1304 переводят в "заблокированное состояние". То есть необходимо разблокирование финансовых инструментов посредством телефонного звонка в центр обслуживания (оператору 1306 сети мобильной

связи или в финансовое учреждение (например, в банк 1314 или FSP 1310), или посредством обоих этих телефонных звонков).

3.2) Операции проверки существования предоставленной SIM-карты: если эта проверка является неуспешной, то финансовые инструменты переводят в "состояние приостановки". То есть финансовые инструменты станут доступными для использования после того, как предоставленная SIM-карта 1308 снова будет доступной.

3.3) Операции проверки возможности установления связи с внутренними службами МЕР (встроенных мобильных платежей) (например, с TIM 400, с FSP 1310). TIM 400 может являться частью инфраструктуры FSP 1310 для обеспечения поддержки платежей в бытовых электронных устройствах, таких как, например, мобильные телефоны 1304.

3.4) Операции проверки возможности установления связи 1305 с собственной сетью 1306 мобильной связи: если эта проверка является неуспешной, то финансовые инструменты переводят в "состояние с ограничением по максимальной сумме". То есть принудительно устанавливается заданную максимальную сумму транзакции (равную, например, 20\$), и транзакции на сумму свыше этой величины не допускают до того момента или тех пор, пока не станут доступными результаты всех важных проверок (например, существования предоставленной SIM-карты 1308, соединения 1309 с внутренними службами МЕР (например, с TIM 400), соединения 1305 с собственной сетью мобильной связи 1306).

3.5) Частота вышеупомянутых механизмов проверки по импульсам может быть отрегулирована системой 1300 МЕР (например, TIM 400, FSP 1310). Кроме того, она может зависеть от профиля риска, поставленного в соответствие пользователю, мобильному телефону 1304 и местоположению (определенному, например, с использованием способов определения географического местоположения при помощи GPS), из которого инициированы транзакции.

TRAA не является строго ограниченными мобильными устройствами, такими как, например, мобильный телефон 1304, и также может быть полезным для других бытовых электронных устройств, в том числе, например, для телевизоров, поддерживающих технологию приема телевизионных трансляций через сеть Интернет (NetTVs), и для бытовых электронных приборов с управлением через компьютерную сеть (NetTops), для которых вместо SIM-карты 1308 может использоваться иной доступный, однозначно идентифицируемый элемент сетевой связи.

На чертеже фиг. 14 изображен пример визуального индикатора 1402 интерактивного обнаружения фишинга (IPD) согласно варианту осуществления настоящего изобретения. Важным аспектом любой открытой модели, например, модели сети Интернет, по определению является то, что приложения могут быть написаны кем угодно; а не только первоисточником. То есть сам факт того, что жизнеспособное коммерческое предприятие предлагает на своем веб-сайте законные услуги, не мешает злоумышленникам представляться подлинным веб-сайтом и собирать параметры доступа пользователей. Этот артефакт открытых моделей ставит важную задачу защиты, которая состоит в том, как идентифицировать и остановить мошенническое приложение. Важной категорией мошеннического программного обеспечения являются фишинг-приложения. Фишинг определен как способ, в котором предпринимают попытки сбора конфиденциальной информации, например, параметров доступа пользователей (например, имени пользователя, пароля или подробной информации о кредитной карте), маскируясь под заслуживающий доверия субъект. Борьба с фишингом является нетривиальной задачей, для решения которой могут потребоваться взаимодействие и участие множества субъектов на различных уровнях экономической системы. Поскольку

эта задача является распределенной, то имеет смысл, чтобы решения также были распределенными аналогичным образом.

Предотвращение фишинга является чрезвычайно сложной задачей, имеющей как технические, так и социально-технические грани. Определение того, является ли приложение мошенническим, или, иными словами, неправомочным выполнять действие, является нетривиальной задачей, которая зависит от многих факторов, таких как, например, операционная система (OS) и программная платформа (также именуемая стеком), на которой работает приложение, структура его интерфейса пользователя (UI), модель его взаимодействия с другими приложениями и службами, и от многих других факторов. Определение самого жулика также является очень общим и неточным. На абстрактном уровне решение задачи борьбы с фишингом эквивалентно распознаванию и разрешению функционирования подлинного приложения (и, следовательно, разрешения ему производить сбор данных о вышеупомянутых параметрах доступа) и в то же самое время распознаванию и запрету функционирования мошеннического приложения, которое выдает себя за подлинное приложение. Следовательно, важно определить цель решения.

Основная цель решения может быть определена как интерактивное обнаружение фишинга (IPD). Как показано на чертеже фиг.4B, любая из систем 500, 600, 700 и 800 MEP может включать в себя модуль 4704 IPD в качестве части TIM 400. В этом техническом решении (например, в варианте реализации посредством модуля 4704 IPD) не предпринимают попытку предотвращения фишинга, поскольку это потребовало бы перечисления всех возможных фишинговых атак, что практически невозможно. Таким образом, объем технического решения дополнительно ограничен следующим образом: А) пользователям предоставлена возможность надежно определять, является ли приложение подлинным; и В) функции IPD инициирует конечный пользователь, который намеревается проверить подлинность приложения. Ограничения А и В означают, что решение основано на намерении пользователя, и что вызов IPD (например, посредством модуля 4704 IPD содержащегося в модуле 470 управления устройством) необязательно является автоматическим. Одним из примеров практического использования IPD является доказательство подлинности средства FSP, обеспечивающего платежи, встроенного в другое приложение, в котором требуются платежные функции.

Вариант осуществления IPD может включать в себя два компонента: клиентский компонент (например, мобильный телефон 510) и серверный компонент (например, TIM 400, включающий в себя модуль 4704 IPD). Клиентский компонент находится в целевом устройстве (например, в мобильном телефоне 510, персональном компьютере, портативном компьютере, телефонной трубке мобильной связи), которое удовлетворяет следующим общим требованиям: 1) осведомлено о сети; 2) само является заслуживающим доверия; 3) содержит элемент UI (интерфейс пользователя); 4) имеет средство проверки подлинности; 5) может быть встроенным или автономным; 6) степень доверия к нему может быть проверена (то есть может быть выполнена аутентификация).

Клиентский компонент (например, мобильный телефон 510) именуют "основой доверия" (Trust Base), поскольку он способен создавать и проверять доверительное утверждение (то есть оно не является фальсифицированным). На высоком уровне и с упомянутыми выше характеристиками основа доверия гарантирует то, что при выполнении приложения и во время получения им параметров доступа пользователей (и если пользователь выбрал это) может быть проверена подлинность всех элементов, участвующих в этом процессе. Если эта проверка является неуспешной, то пользователя уведомляют об этом посредством визуального индикатора, обеспеченного элементом

UI, который, в свою очередь, указывает возможную попытку фишинга.

Серверный компонент (например, ТИМ 400, включающий в себя модуль 4704 IPD) именуют "источником доверия" (Trust Source), поскольку он случайным образом генерирует информацию о проверке подлинности, которая может быть получена клиентским компонентом, и также может быть визуально проверена пользователем. Например, как видно на чертеже фиг.14, информация о проверке подлинности может представлять собой кнопку красного цвета или иного цвета, или затемненную кнопку с трехзначным числом в ней, образуя визуальный индикатор 1402 IPD.

В качестве примера визуального индикатора 1402 IPD цвет клавиши и числа в ней изменяются случайным образом и периодически. Эта клавиша визуального индикатора 1402 IPD показана, например, в стандартном месте на веб-сайте "источника доверия" (например, на веб-сайте FSP 1310).

Один из вариантов реализации IPD работает следующим образом. Когда пользователь принимает решение о проверке того, является ли сомнительное программное обеспечение подлинным, то:

1) Пользователь делает щелчок на кнопке "проверить" (имеющийся, например, на компоненте UI клиента 510);

2) Кнопка "проверить" заставляет средство проверки подлинности выполнить аутентификацию клиента 510 для сервера 400;

3) После успешной аутентификации клиента 510 сервером 400:

а) Средство проверки подлинности, имеющееся у клиента 510, извлекает из сервера 400 текущие установки цвета (для кнопки и для числа) визуального индикатора 1402 IPD, а также числовое значение для него;

б) Компонент UI клиента 510 показывает кнопку с установкой цвета визуального индикатора 1402 IPD и число на нем, которые извлечены средством проверки подлинности, имеющимся у клиента 510.

4) Пользователь посещает сайт "источника доверия" (например, веб-сайт FSP 1310) и проверяет, что цвет визуального индикатора IPD 1402 и число на нем, которые показаны посредством кнопки "проверить" клиентского компонента 510 у пользователя, являются теми же самыми, что и на кнопке, отображенной на сайте "источника доверия".

Серверный компонент (например, ТИМ 400) отвечает только подлинному клиентскому компоненту (например, мобильному телефону 510), поскольку имеется операция аутентификации, затребованная сервером (например, ТИМ 400) для того, чтобы послать любой ответ. Мошенническое приложение было бы не способным пройти аутентификацию, и может только попытаться отгадать правильную комбинацию цветов и чисел. Поскольку эта комбинация установлена в сервере (например, в ТИМ 400 веб-сайта "источника доверия", которым является FSP 1310) случайным образом, а также периодически изменяется, то удобный момент для мошеннического приложения является строго ограниченным.

При реализации различных вариантов осуществления изобретения варианты осуществления настоящего изобретения могут содержать персональное вычислительное устройство, например, персональный компьютер, портативный компьютер, персональное цифровое информационное устройство (PDA), сотовый телефон или другие персональные вычислительные устройства или устройства связи. Система поставщика платежных услуг может содержать сетевое вычислительное устройство, например, сервер или множество серверов, компьютеров или устройств обработки, объединенных так, что они определяют компьютерную систему или сеть для предоставления платежных услуг, обеспечиваемых системой поставщика платежных

услуг.

В этом отношении компьютерная система может включать в себя шину или иное средство связи для передачи информации, которое соединяет между собой подсистемы и компоненты, такие как, например, компонент обработки (например, процессор, микроконтроллер, устройство цифровой обработки сигналов (DSP) и т.д.), компонент, представляющий собой системную память, (например, оперативное запоминающее устройство (RAM)), компонент, представляющий собой статическое запоминающее устройство (например, постоянное запоминающее устройство (ROM)), компонент, представляющий собой накопитель на дисках (например, магнитных или оптических), компонент, представляющий собой сетевой интерфейс (например, модем или карта стандарта Ethernet), компонент, представляющий собой дисплей, (например, дисплей с электронно-лучевой трубкой (CRT) или жидкокристаллический дисплей (LCD)), компонент, представляющий собой устройство ввода, (например, клавиатура или кнопочная панель) и/или компонент управления курсором (например, манипулятор типа "мышь" или шаровой манипулятор). В одном из вариантов осуществления изобретения компонент, представляющий собой накопитель на дисках, может содержать базу данных, имеющую один или большее количество компонентов, представляющих собой накопители на дисках.

Компьютерная система может выполнять конкретные операции посредством процессора и выполнять одну или большее количество последовательностей из одной или большего количества команд, содержащихся в компоненте, представляющем собой системную память. Такие команды могут быть считаны в компонент, представляющий собой системную память, с другого считываемого посредством компьютера носителя информации, например, из компонента, представляющего собой статическое запоминающее устройство, или из компонента, представляющего собой накопитель на дисках. В других вариантах осуществления изобретения для реализации изобретения вместо программных команд или в сочетании с ними могут использоваться проводные схемы.

Логика может быть закодирована в считываемом посредством компьютера носителе информации, который может относиться к любому носителю информации, который участвует в подаче команд в процессор для их выполнения. Такой носитель информации может представлять собой носитель информации множества типов, которыми являются, в том числе, энергонезависимые носители информации, энергозависимые носители информации и передающие среды, но эти примеры не являются ограничивающим признаком. В различных вариантах реализации энергонезависимый носитель информации включает в себя оптические или магнитные диски, например, компонент, представляющий собой накопитель на дисках, энергозависимый носитель информации включает в себя динамическую память, например, компонент, представляющий собой системную память, а передающие среды включают в себя коаксиальные кабели, медный провод и волоконную оптику, в том числе, провода, которые содержат шину. В одном из примеров среды передачи могут иметь вид акустических или световых волн, например, сгенерированных во время передачи данных посредством радиоволн и инфракрасного излучения.

Некоторыми обычными разновидностями считываемых посредством компьютера носителей информации являются, в том числе, например, дискета, гибкий диск, накопитель на жестких дисках, магнитная лента, любой другой магнитный носитель, постоянное запоминающее устройство на компакт-диске (CD-ROM), любой другой оптический носитель, перфокарты, перфолента, любой другой физический носитель со

структурой отверстий, оперативное запоминающее устройство (RAM), постоянное запоминающее устройство (ROM), стираемое программируемое постоянное запоминающее устройство (EPROM), FLASH-EPROM, любая другая микросхема или картридж запоминающего устройства, несущая волна или любой другой носитель информации, под который приспособлен компьютер.

В различных вариантах осуществления изобретения выполнение последовательностей команд для практической реализации изобретения может осуществлять компьютерная система. В различных других вариантах осуществления изобретения последовательности команд для практической реализации изобретения может выполнять множество компьютерных систем, связанных линией связи (например, локальной сетью (LAN), беспроводной локальной сетью (WLAN), коммутируемой телефонной сетью общего пользования (PSTN) или различными иными сетями проводной или беспроводной связи) согласованно друг с другом.

Компьютерная система может передавать и принимать сообщения, данные, информацию и команды, включающие в себя одну или большее количество программ (то есть прикладных программ) через линию связи и интерфейс связи. Принятый программный код может быть выполнен процессором в принятом виде и/или может быть сохранен в компоненте, представляющем собой накопитель на дисках, или в каком-либо ином компоненте, представляющем собой энергонезависимое запоминающее устройство, для его выполнения.

Где уместно, различные варианты осуществления изобретения, предложенные в настоящем изобретении, сущность которого здесь раскрыта, могут быть реализованы с использованием аппаратных средств, программного обеспечения или комбинации аппаратных средств и программного обеспечения. К тому же, где уместно, описанные здесь различные аппаратные компоненты и/или программные компоненты могут быть объединены в составные компоненты, содержащие программное обеспечение, аппаратные средства и/или оба эти средства, не выходя за пределы сущности настоящего изобретения, которое здесь раскрыто. Где уместно, описанные здесь различные аппаратные компоненты и/или программные компоненты могут быть разделены на субкомпоненты, содержащие программное обеспечение, аппаратные средства или оба эти средства, не выходя за пределы объема настоящего изобретения, сущность которого здесь раскрыта. Кроме того, где уместно, предполагают, что программные компоненты могут быть реализованы как аппаратные компоненты и, наоборот.

Согласно настоящему изобретению, сущность которого здесь раскрыта, программное обеспечение, например, программный код и/или данные, может быть сохранено на одном или на большем количестве считываемых посредством компьютера носителях информации. Также предполагают, что описанное здесь программное обеспечение может быть реализовано с использованием одного или большего количества универсальных компьютеров или специализированных компьютеров и/или компьютерных систем с сетевой и/или с иной структурой. Где уместно, описанный здесь порядок выполнения различных операций может быть изменен, они могут быть объединены в составные операции и/или разделены на подоперации для обеспечения описанных здесь признаков.

Подразумевают, что приведенное выше описание изобретения не ограничивает настоящее изобретение точными его вариантами или конкретными областями его применения, которые здесь раскрыты. Полагают, что с учетом описания изобретения возможны различные альтернативные варианты осуществления изобретения и/или видоизменения настоящего изобретения вне зависимости от того, описаны ли здесь они

в явном виде или подразумеваются. Таким образом, зная различные варианты осуществления изобретения из описания, которые приведены в качестве примеров, для специалистов со средним уровнем компетентности в данной области техники понятно, что могут быть произведены изменения, касающиеся формы и подробностей, не выходя за пределы объема настоящего изобретения. Таким образом, изобретение ограничено только лишь формулой изобретения.

Формула изобретения

1. Система безопасных платежей для использования доверенным администратором обслуживания (TSM) и с мобильным устройством, имеющим уникальные идентификационные данные, содержащая:

серверное устройство обработки данных, при этом:

серверное устройство обработки данных принимает приложение от доверенного администратора обслуживания (TSM) в ответ на запрос, сделанный пользователем доверенному поставщику услуг (TSP) доверенного администратора обслуживания (TSM), на активацию платежных функций в мобильном устройстве, и

серверное устройство обработки данных аутентифицирует данное приложение и предоставляет аутентифицированное приложение доверенной третьей стороне (ТТР), и доверенная третья сторона (ТТР) по радиосвязи (ОТА) устанавливает аутентифицированное приложение в мобильное устройство; и

защищенный элемент (SE), действующий в качестве клиента, при этом:

защищенный элемент (SE) присутствует в мобильном устройстве в качестве клиента;

защищенный элемент (SE) устанавливает аутентифицированное приложение из серверного устройства обработки данных в защищенном элементе (SE);

защищенный элемент (SE) приспособлен для исполнения аутентифицированного приложения для выполнения процедуры обслуживания во взаимодействии с серверным устройством обработки данных и доверенным администратором обслуживания (TSM), при этом:

процедура обслуживания включает в себя активацию платежных функций в мобильном устройстве, причем активация платежных функций включает в себя:

обеспечение защищенной связи между мобильным устройством и доверенным администратором обслуживания (TSM); и

защищенное снабжение мобильного устройства платежным средством, включая предоставление информации о платежном средстве от серверного устройства обработки данных в мобильное устройство, при этом:

серверное устройство обработки данных уведомлено от доверенного поставщика услуг (TSP) доверенного администратора обслуживания (TSM), что денежные средства пользователя доступны для платежного средства со счета пользователя, в ответ на запрос, сделанный пользователем доверенному администратору обслуживания (TSM), на снабжение платежным средством,

информация о платежном средстве посылается из серверного устройства обработки данных доверенной третьей стороне (ТТР), и

доверенная третья сторона (ТТР) по радиосвязи (ОТА) устанавливает платежное средство в защищенный элемент (SE) в мобильном устройстве, так что мобильное устройство становится способным действовать в качестве платежного средства.

2. Система по п.1, дополнительно содержащая:

второе устройство, имеющее аппаратно-защищенное запоминающее устройство и метку;

идентификатор метки, который считывается с метки и сохраняется в содержимом аппаратно-защищенного запоминающего устройства во втором устройстве,

при этом мобильное устройство сконфигурировано для считывания идентификатора метки, так что если найдено соответствие между идентификатором метки и содержимым аппаратно-защищенного запоминающего устройства, то идентификатор метки заслуживает доверия как отражающий подлинность второго устройства.

3. Система по п.1, в которой аутентификация мобильного устройства серверным средством обработки данных основана на доказательстве с нулевым разглашением, дополненном аппаратной защитой информации о секретном ключе.

4. Система по п.1, дополнительно содержащая доверенный дистанционный удостоверяющий агент (TRAA), сконфигурированный для выполнения набора шагов проверки по импульсам для гарантии того, что чувствительное к защите соединение между защищенным элементом (SE), действующим в качестве клиента и присутствующим в мобильном устройстве, и серверным средством обработки данных имеется и является действующим.

5. Система по п.1, дополнительно содержащая интерактивный визуальный индикатор обнаружения фишинга, извлеченный мобильным устройством после успешной аутентификации клиента мобильного устройства серверным средством обработки данных, при этом интерактивный визуальный индикатор обнаружения фишинга доступен на сайте источника доверия для сопоставления пользователем мобильного устройства извлеченного визуального индикатора и визуального индикатора, доступного на сайте источника доверия.

6. Способ регистрации для выполнения финансовой транзакции из мобильного устройства во взаимодействии с доверенным администратором обслуживания (TSM), содержащий этапы, на которых:

посредством сервера через доверенного поставщика услуг (TSP) доверенного администратора обслуживания (TSM) принимают выполненный посредством мобильного устройства запрос пользователя на активацию платежных функций в мобильном устройстве;

активируют платежные функции в мобильном устройстве посредством сервера во взаимодействии с доверенным администратором обслуживания (TSM), при этом: сервер аутентифицирует приложение;

сервер предоставляет аутентифицированное приложение доверенной третьей стороне (ТТР), и доверенная третья сторона (ТТР) по радиосвязи (ОТА) устанавливает аутентифицированное приложение в мобильное устройство; и

аутентифицированное приложение устанавливают во встроенном защищенном элементе (SE) мобильного устройства;

исполняют аутентифицированное приложение в защищенном элементе (SE) мобильного устройства для запрашивания у доверенного поставщика услуг (TSP) доверенного администратора обслуживания (TSM) снабдить мобильное устройство платежным средством;

посредством доверенного поставщика услуг (TSP) доверенного администратора обслуживания (TSM) запрашивают у банка подтверждение денежных средств пользователя для платежного средства, запрошенного для мобильного устройства, причем мобильное устройство идентифицируется по идентификационным данным абонента;

в ответ на разрешение из банка, принятое доверенным администратором обслуживания (TSM), и уведомление доверенным администратором обслуживания

(TSM) сервера о том, что денежные средства пользователя доступны для платежного средства со счета пользователя, посредством сервера проверяют подлинность информации о платежном средстве и упаковывают ее для активации платежного средства в надлежащем формате для встроенного защищенного элемента (SE) мобильного

5 устройства;

передают упакованную информацию о платежном средстве из сервера доверенной третьей стороне (ТТР); и

посредством доверенной третьей стороны (ТТР) устанавливают по радиосвязи (OTA) упакованную информацию о платежном средстве во встроенный защищенный

10 элемент (SE) мобильного устройства, так что мобильное устройство становится способным действовать в качестве платежного средства.

7. Способ по п.6, дополнительно содержащий этапы, на которых:

посредством встроенного защищенного элемента (SE) проверяют, имеется ли в мобильном устройстве предоставленная карта модуля идентификации абонента (SIM);

15 и

в качестве реакции на отсутствие предоставленной SIM карты в мобильном устройстве делают платежное средство мобильного устройства недоступным для использования.

8. Способ по п.6, дополнительно содержащий этап, на котором посредством сервера

20 используют множество данных, связанных с абонентом и с мобильным устройством, для проверки подлинности, времени, географического местоположения или учетных данных авторизации при транзакциях в процедуре эквайринга с использованием канала беспроводной связи мобильного устройства во взаимодействии с обычной сетью эквайринга.

9. Способ по п.6, дополнительно содержащий этап, на котором используют идентификационные данные абонента для управления допустимым уровнем риска, где этот риск связан с использованием мобильного устройства.

10. Способ по п.6, дополнительно содержащий этапы, на которых:

создают профиль для мобильного устройства; и

30 используют этот профиль для управления рисками, связанными с использованием мобильного устройства в автономном режиме.

11. Способ по п.6, дополнительно содержащий этап, на котором выполняют набор шагов проверки по импульсам для гарантии того, что чувствительное к защите соединение имеется и является действующим.

35 12. Способ по п.6, дополнительно содержащий этап, на котором:

посредством мобильного устройства извлекают интерактивный визуальный индикатор обнаружения фишинга после успешной аутентификации клиента мобильного устройства сервером; и

40 делают интерактивный визуальный индикатор обнаружения фишинга доступным на сайте источника доверия для сопоставления пользователем мобильного устройства извлеченного визуального индикатора и визуального индикатора, доступного на сайте источника доверия.

13. Способ по п.6, дополнительно содержащий этап, на котором аутентифицируют мобильное устройство посредством сервера на основе доказательства с нулевым разглашением, дополненного аппаратной защитой информации о секретном ключе.

45

14. Способ по п.6, дополнительно содержащий этапы, на которых:

сохраняют идентификатор метки из метки второго устройства в содержимом аппаратно-защищенного запоминающего устройства, имеющемся во втором устройстве;

считывают идентификатор метки из метки; и
сравнивают идентификатор метки с содержимым аппаратно-защищенного
запоминающего устройства, так что если найдено соответствие между идентификатором
метки и содержимым аппаратно-защищенного запоминающего устройства, то
5 идентификатор метки заслуживает доверия как отражающий подлинность второго
устройства.

15. Невременный машиночитаемый носитель информации, имеющий машиночитаемый
и исполняемый код для предписания процессору выполнять способ, содержащий этапы,
на которых:

10 посредством сервера через доверенного поставщика услуг (TSP) доверенного
администратора обслуживания (TSM) принимают выполненный посредством
мобильного устройства запрос пользователя на активацию платежных функций в
мобильном устройстве;

15 активируют платежные функции в мобильном устройстве посредством сервера во
взаимодействии с доверенным администратором обслуживания (TSM), при этом:

сервер аутентифицирует приложение;

сервер предоставляет аутентифицированное приложение доверенной третьей стороне
(ТТР), и доверенная третья сторона (ТТР) по радиосвязи (ОТА) устанавливает
аутентифицированное приложение в мобильное устройство; и

20 аутентифицированное приложение устанавливают во встроенном защищенном
элементе (SE) мобильного устройства;

исполняют аутентифицированное приложение в защищенном элементе (SE)
мобильного устройства для запрашивания у доверенного поставщика услуг (TSP)
доверенного администратора обслуживания (TSM) снабдить мобильное устройство
25 платежным средством;

30 посредством доверенного поставщика услуг (TSP) доверенного администратора
обслуживания (TSM) запрашивают у банка подтверждение денежных средств
пользователя для платежного средства, запрошенного для мобильного устройства,
причем мобильное устройство идентифицируется по уникальным идентификационным
данным;

35 в ответ на разрешение из банка, принятое доверенным администратором
обслуживания (TSM), и уведомление доверенным администратором обслуживания
(TSM) сервера о том, что денежные средства пользователя доступны для платежного
средства со счета пользователя, посредством сервера проверяют подлинность
информации о платежном средстве и упаковывают ее для активации платежного средства
в надлежащем формате для встроенного защищенного элемента (SE) мобильного
устройства;

передают упакованную информацию о платежном средстве из сервера доверенной
третьей стороне (ТТР); и

40 посредством доверенной третьей стороны (ТТР) устанавливают по радиосвязи
(ОТА) упакованную информацию о платежном средстве во встроенный защищенный
элемент (SE) мобильного устройства, так что мобильное устройство становится
способным действовать в качестве платежного средства.

16. Машиночитаемый носитель по п.15, дополнительно содержащий машиночитаемый
45 код для предписания процессору:

поверять посредством встроенного защищенного элемента (SE), имеется ли в
мобильном устройстве предоставленная карта модуля идентификации абонента (SIM);
и

в качестве реакции на отсутствие предоставленной SIM карты в мобильном устройстве делать платежное средство мобильного устройства недоступным для использования.

5 17. Машиночитаемый носитель по п.15, дополнительно содержащий машиночитаемый код для предписания процессору гарантировать, используя набор шагов проверки по импульсам, что чувствительное к защите соединение имеется и является действующим.

18. Машиночитаемый носитель по п.15, дополнительно содержащий машиночитаемый код для предписания процессору:

10 извлекать посредством мобильного устройства интерактивный визуальный индикатор обнаружения фишинга после успешной аутентификации клиента мобильного устройства сервером; и

15 делать интерактивный визуальный индикатор обнаружения фишинга доступным на сайте источника доверия для сопоставления пользователем мобильного устройства извлеченного визуального индикатора и визуального индикатора, доступного на сайте источника доверия.

19. Машиночитаемый носитель по п.15, дополнительно содержащий машиночитаемый код для предписанию процессору аутентифицировать мобильное устройство посредством сервера на основе доказательства с нулевым разглашением, дополненного аппаратной защитой информации о секретном ключе.

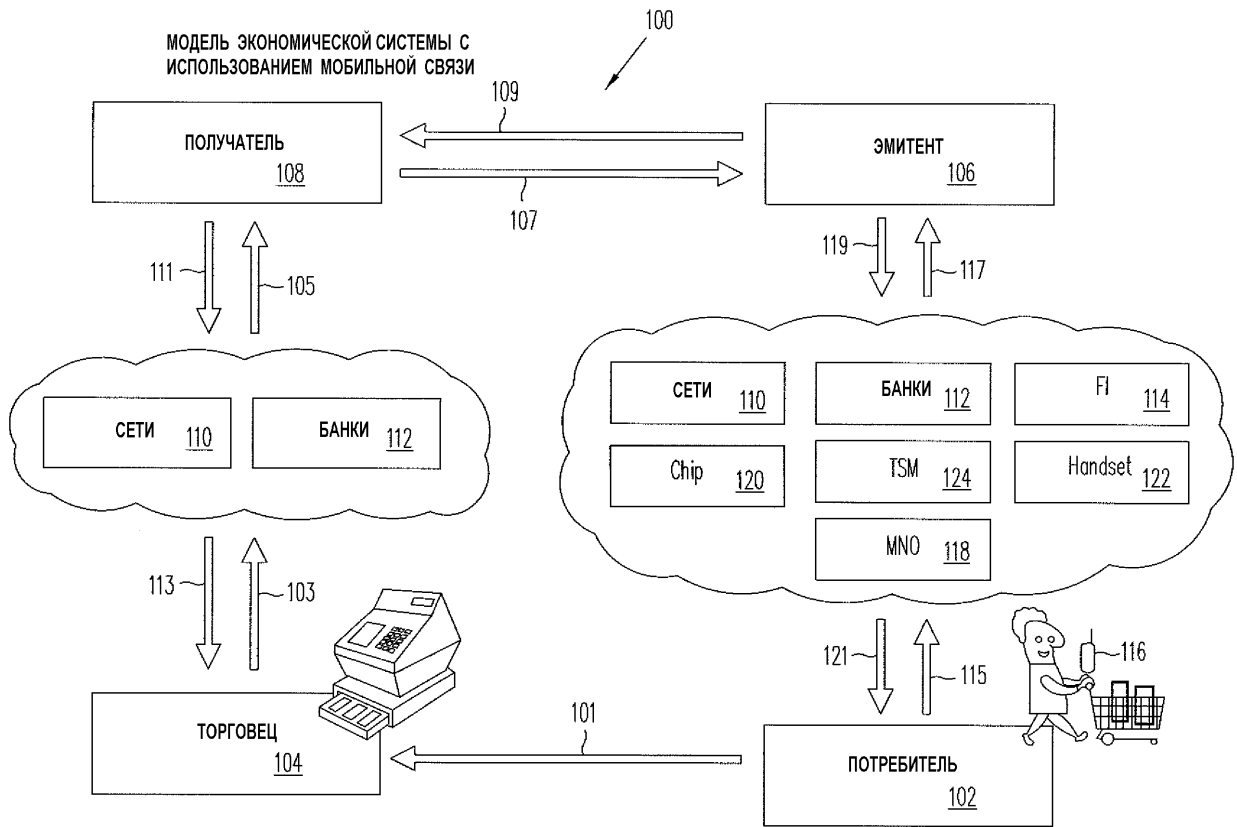
20 20. Машиночитаемый носитель по п.15, дополнительно содержащий машиночитаемый код для предписания процессору выполнять сохранение идентификатора метки из метки второго устройства в содержимом аппаратно-защищенного запоминающего устройства, имеющегося во втором устройстве, с тем чтобы после считывания идентификатора метки из метки и сравнения идентификатора метки с содержимым аппаратно-
25 защищенного запоминающего устройства, если найдено соответствие между идентификатором метки и содержимым аппаратно-защищенного запоминающего устройства, идентификатор метки заслуживал бы доверия как отражающий подлинность второго устройства.

30

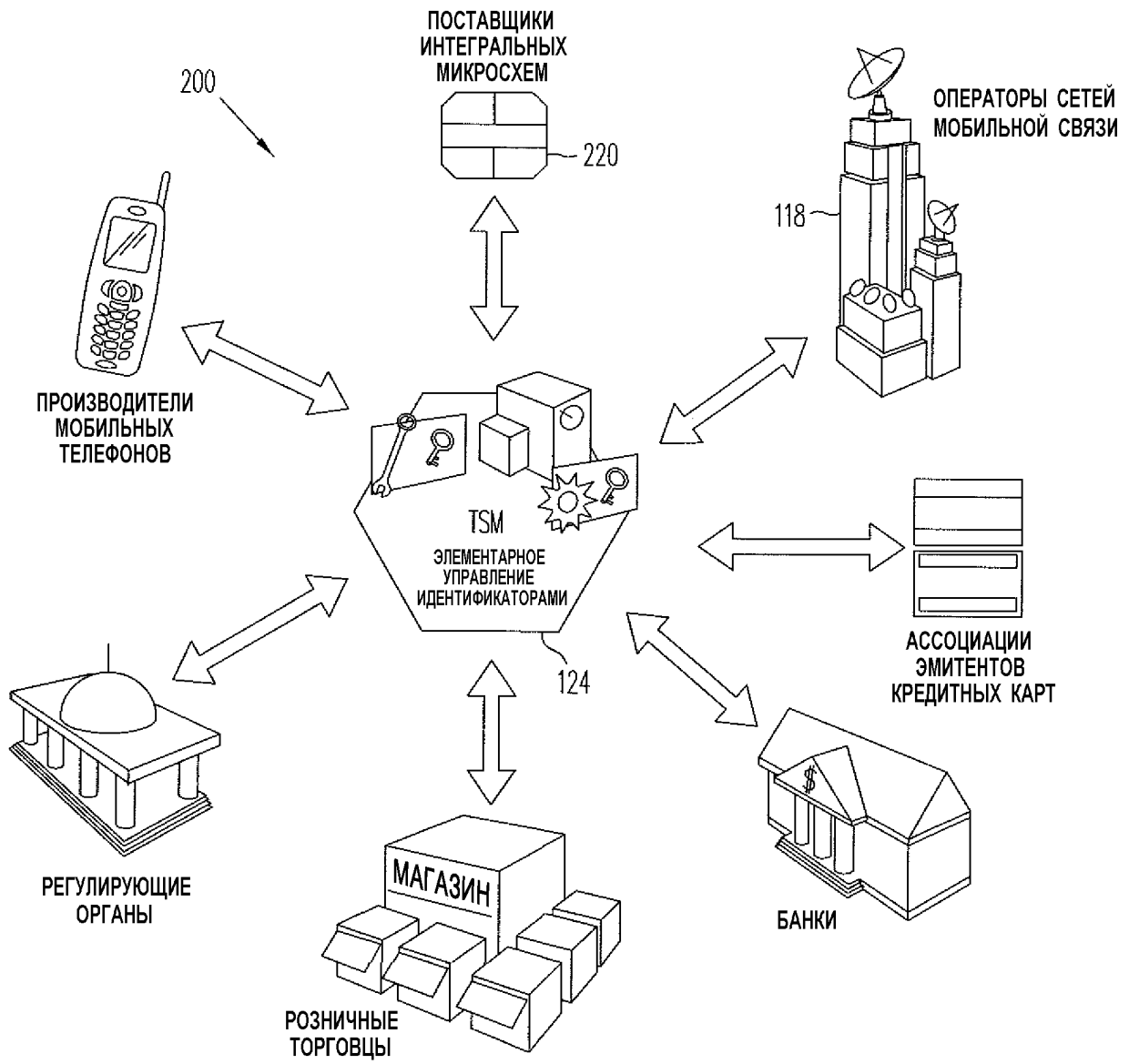
35

40

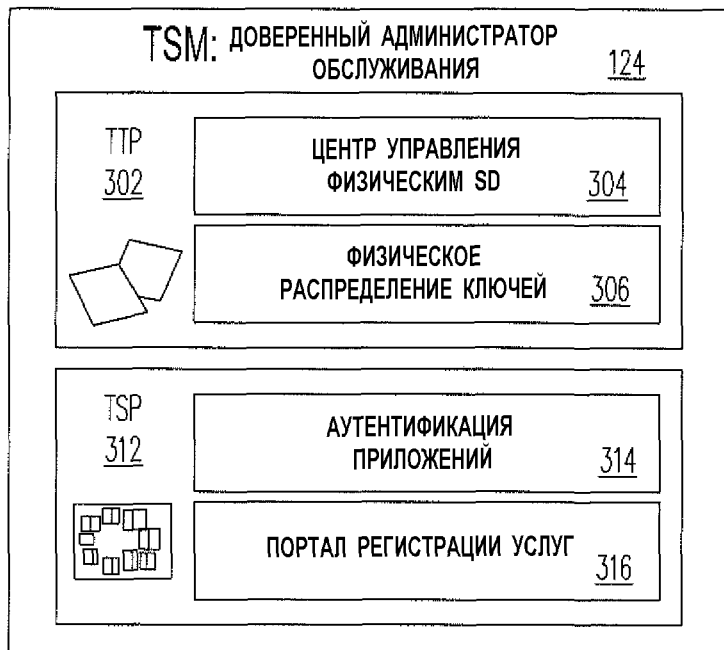
45



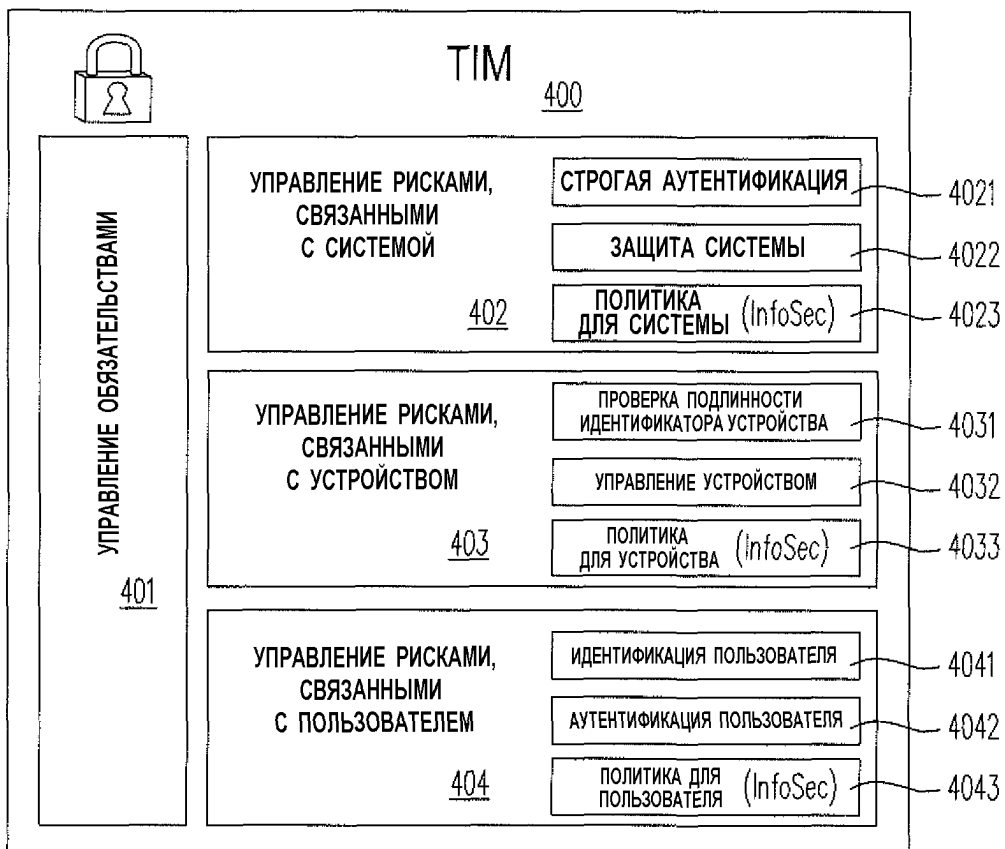
ФИГ.1



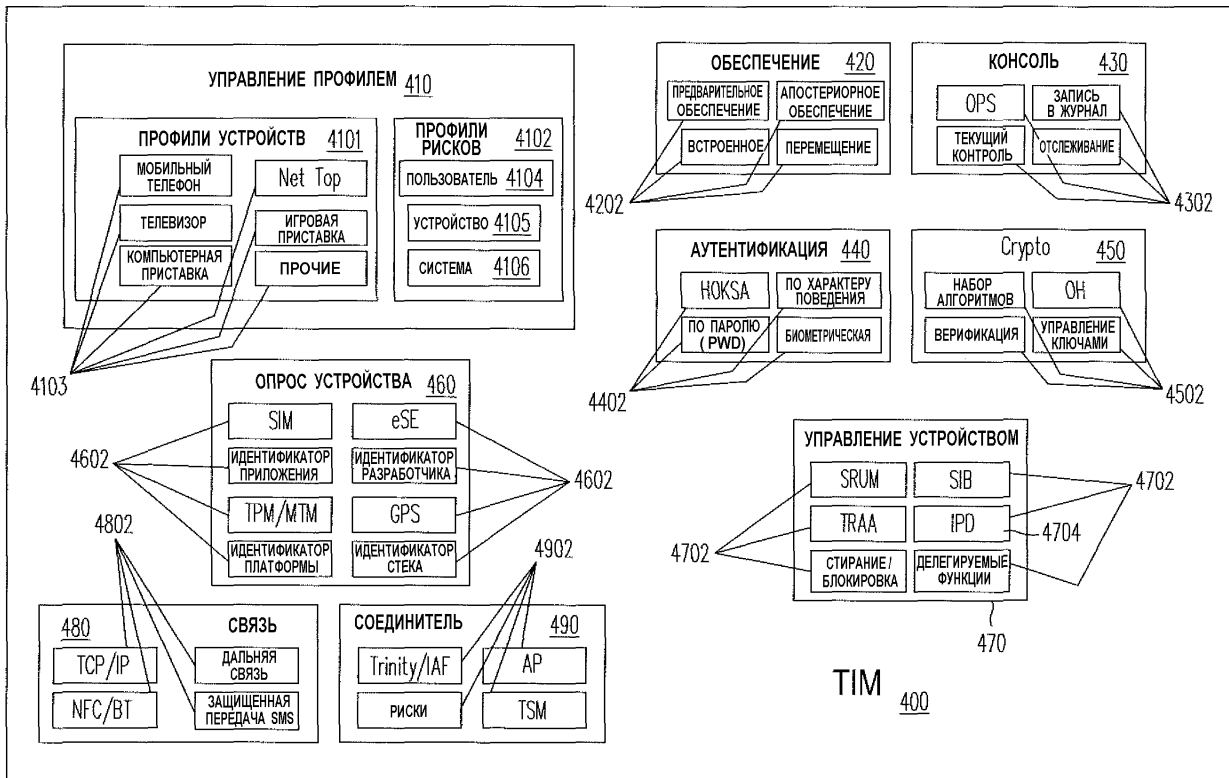
ФИГ.2



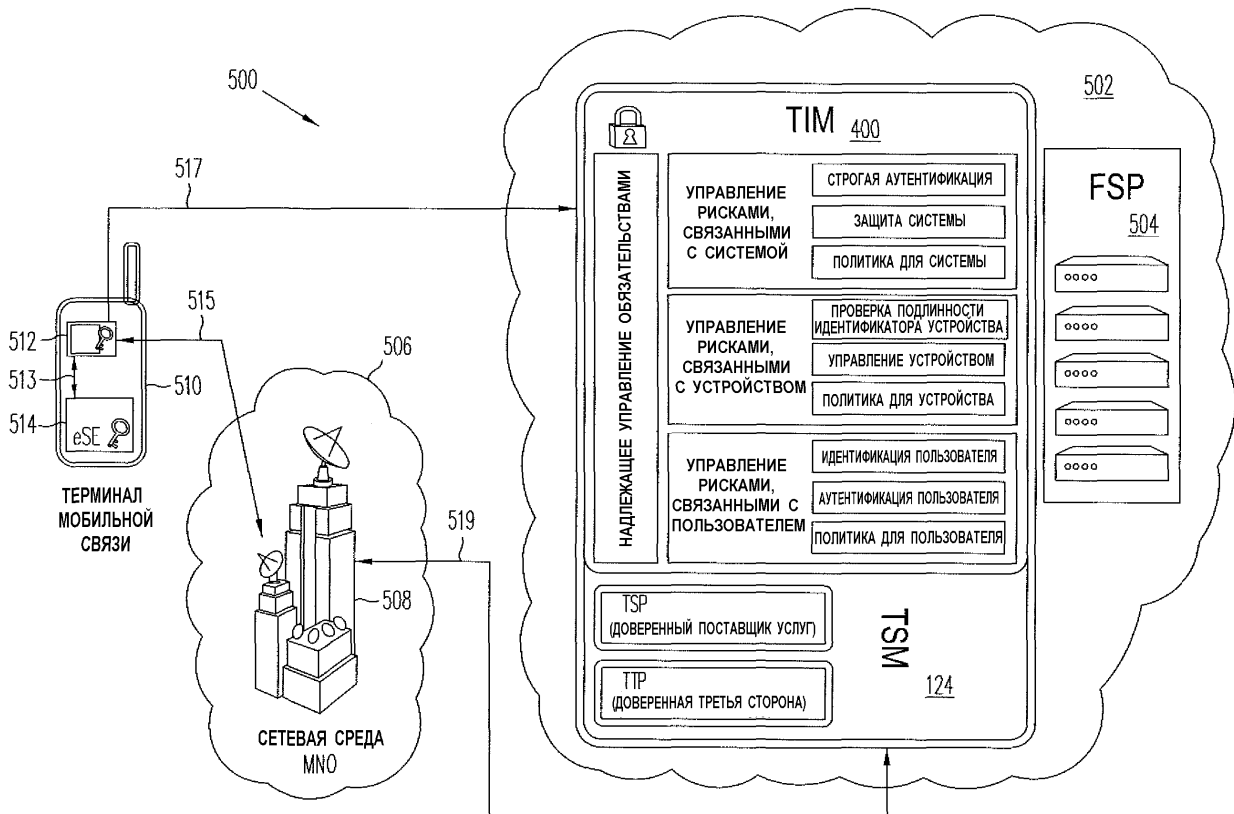
ФИГ.3



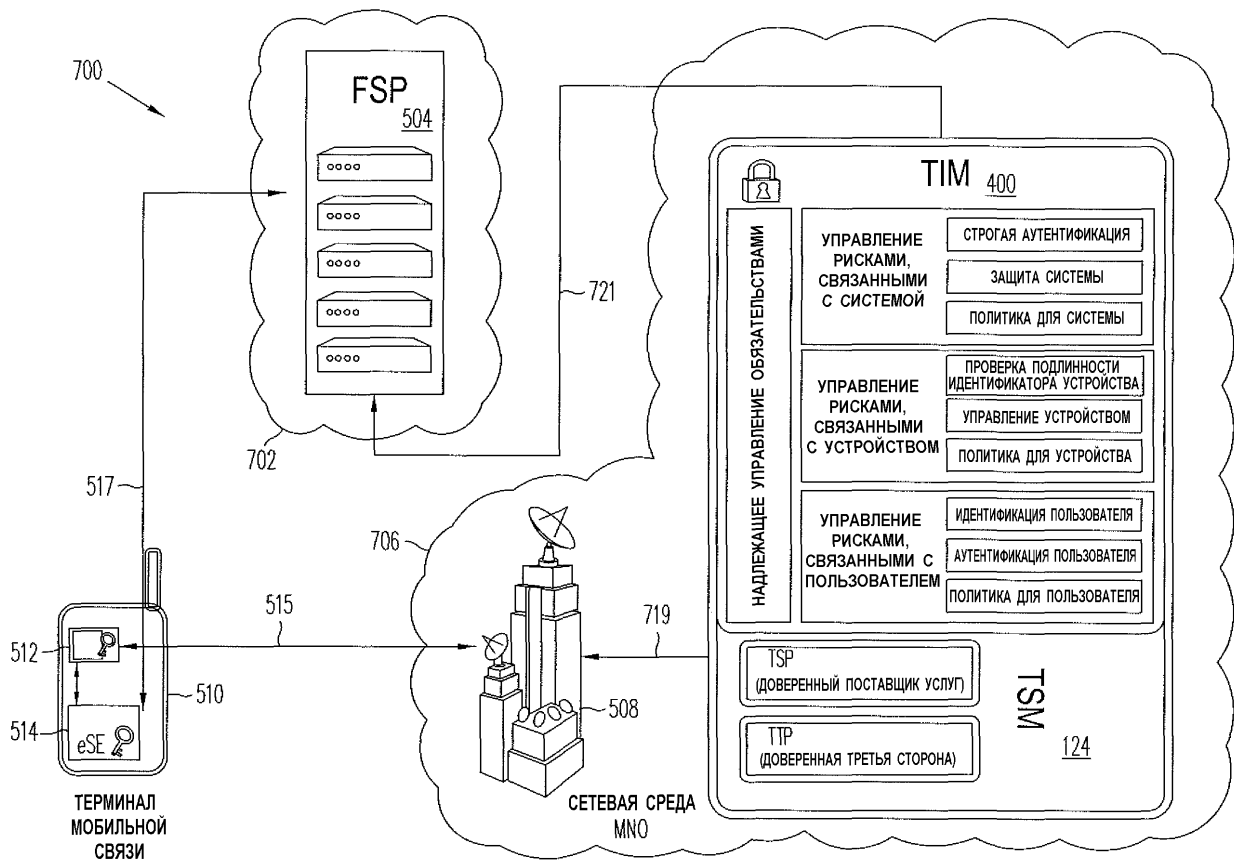
ФИГ.4А



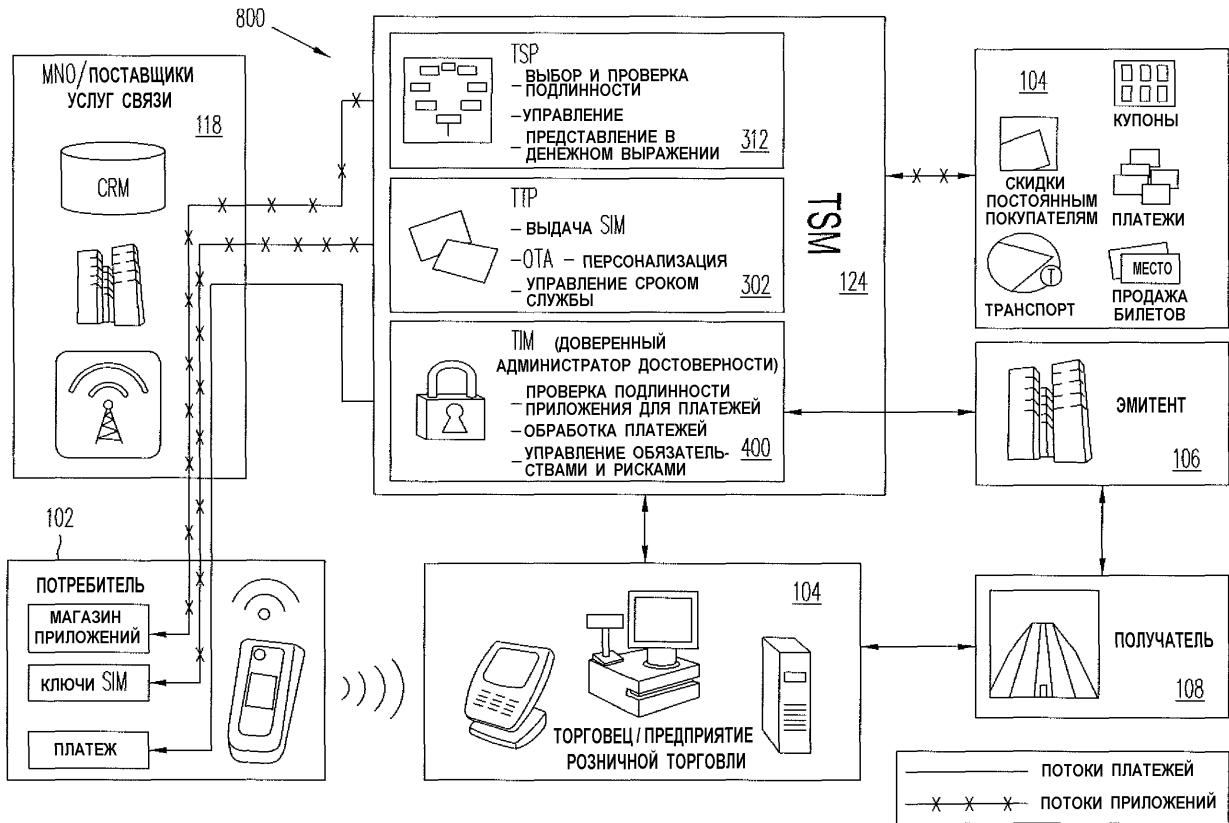
ФИГ.4В



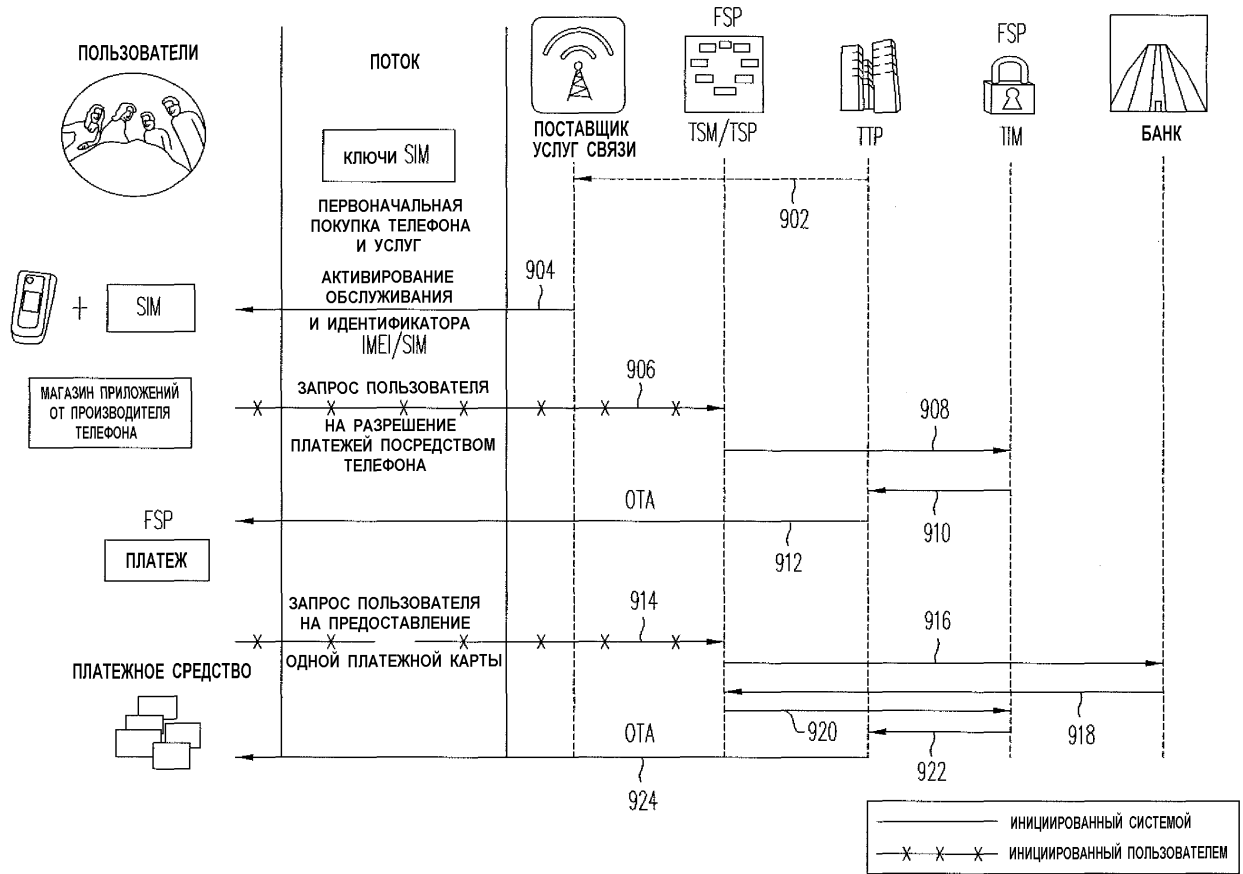
ФИГ.5



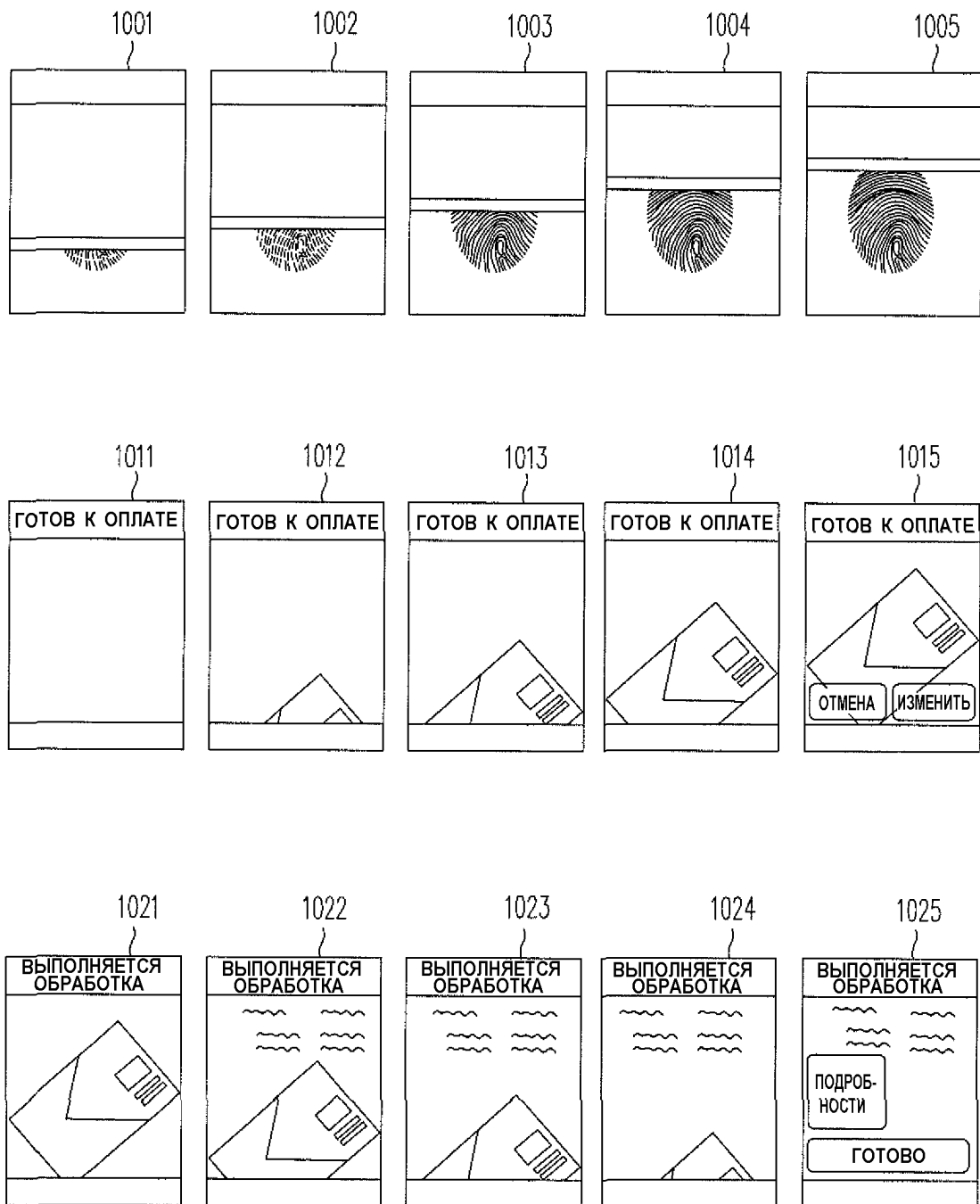
ФИГ.7



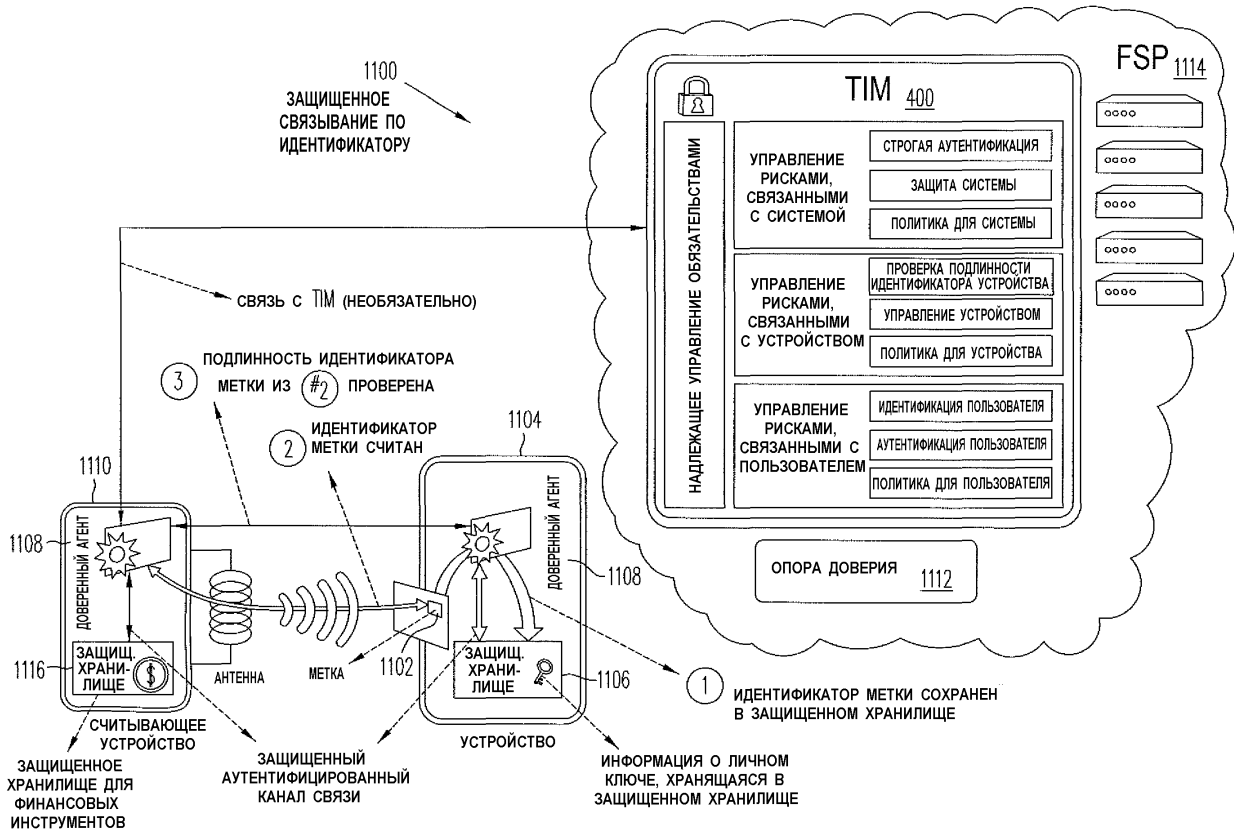
ФИГ.8



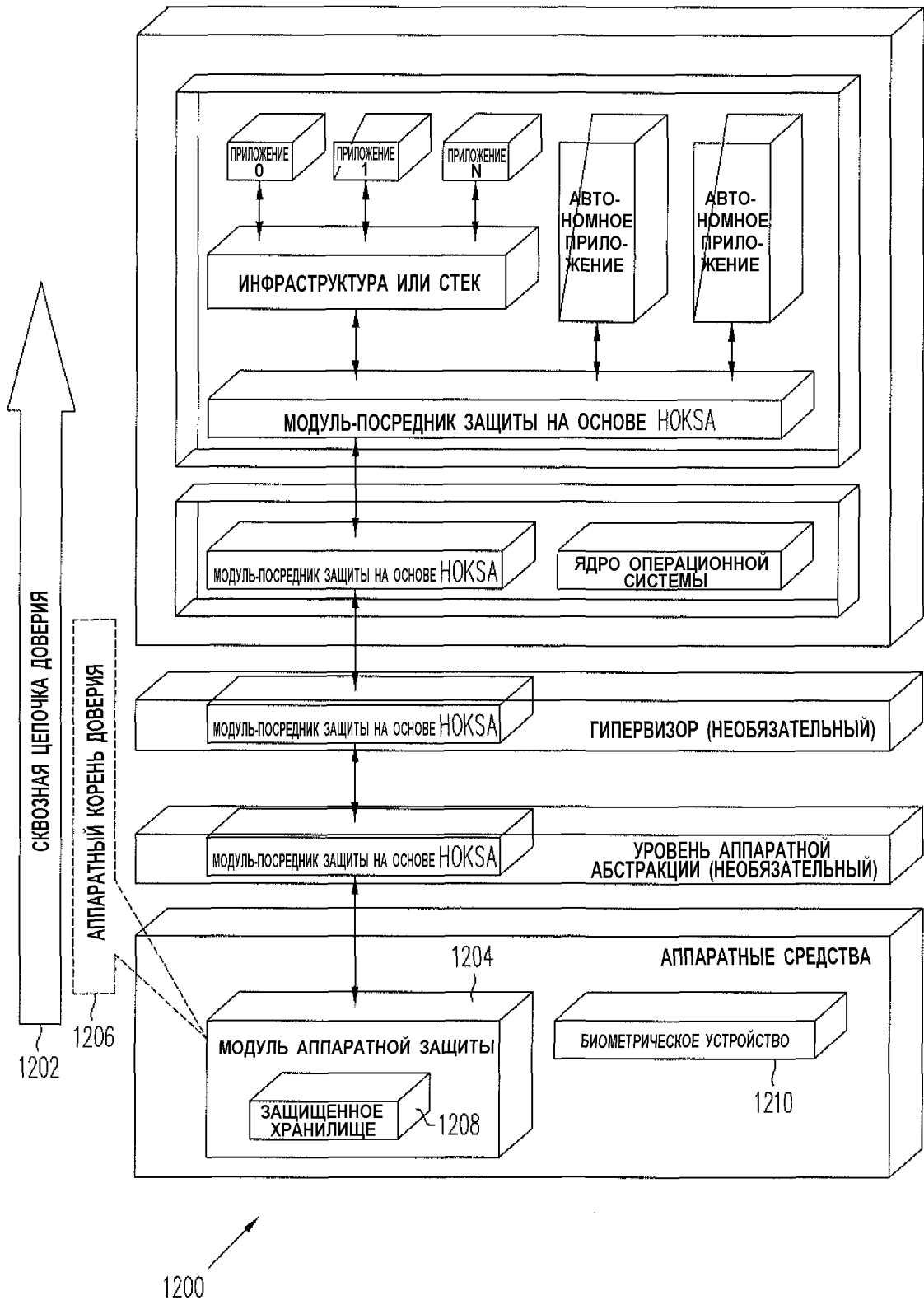
ФИГ.9



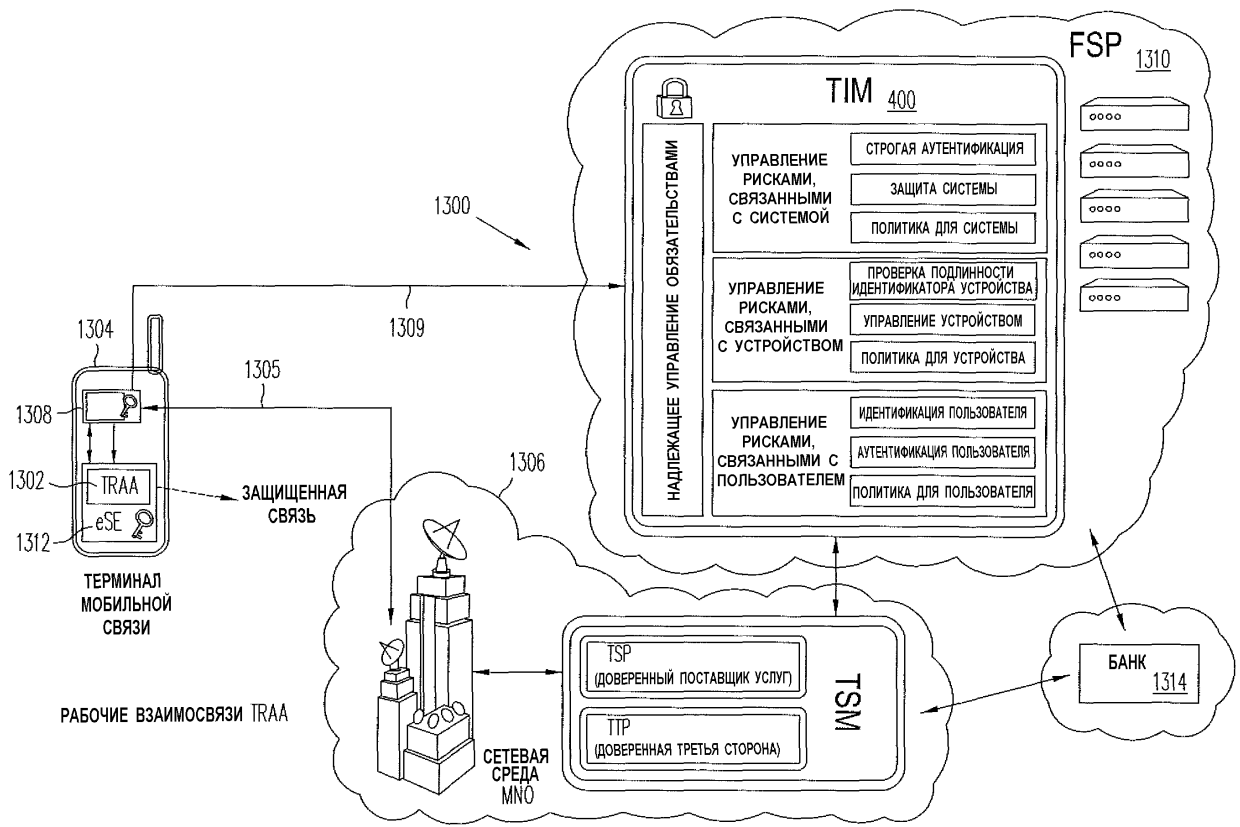
ФИГ.10



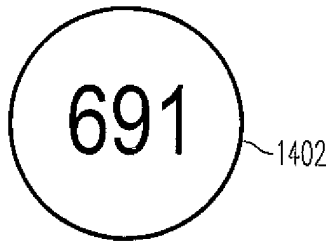
ФИГ.11



ФИГ.12



ФИГ.13



ВИЗУАЛЬНЫЙ ИНДИКАТОР IPD

ФИГ.14