РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 651 245**(13) **C2**

(51) МПК
G06Q 20/32 (2012.01)
G06Q 20/40 (2012.01)
G06Q 20/38 (2012.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06Q 20/3226 (2006.01); G06Q 20/3829 (2006.01); G06Q 20/40 (2006.01)

(21)(22) Заявка: **2015104781, 09.07.2013**

(24) Дата начала отсчета срока действия патента:
09.07.2013

Дата регистрации:
18.04.2018

Приоритет(ы):
(30) Конвенционный приоритет:
13.07.2012 FR 1256779

(43) Дата публикации заявки: **27.08.2016** Бюл. № **24**

(45) Опубликовано: **18.04.2018** Бюл. № **11**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **13.02.2015**

(86) Заявка PCT:
FR 2013/051630 (09.07.2013)

(87) Публикация заявки PCT:
WO 2014/009646 (16.01.2014)

Адрес для переписки:
109012, Москва, ул. Ильинка, 5/2, ООО "Союзпатент"

(72) Автор(ы):
ОБЭН Ян-Лоик (FR),
ДЮКРОС Кристоф (FR),
ДЕПЬЕР Тьерри (FR),
ГОВЭН Давид (FR),
РИКО Рубен (FR)

(73) Патентообладатель(и):
ОБЕРТУР ТЕКНОЛОДЖИ (FR)

(56) Список документов, цитированных в отчете о поиске: **US 2011/0251892 A1, 13.10.2011. EP 2053553 A1, 29.04.2009. US 2011/0265149 A1, 27.10.2011. RU 2008128277 A, 20.01.2010.**

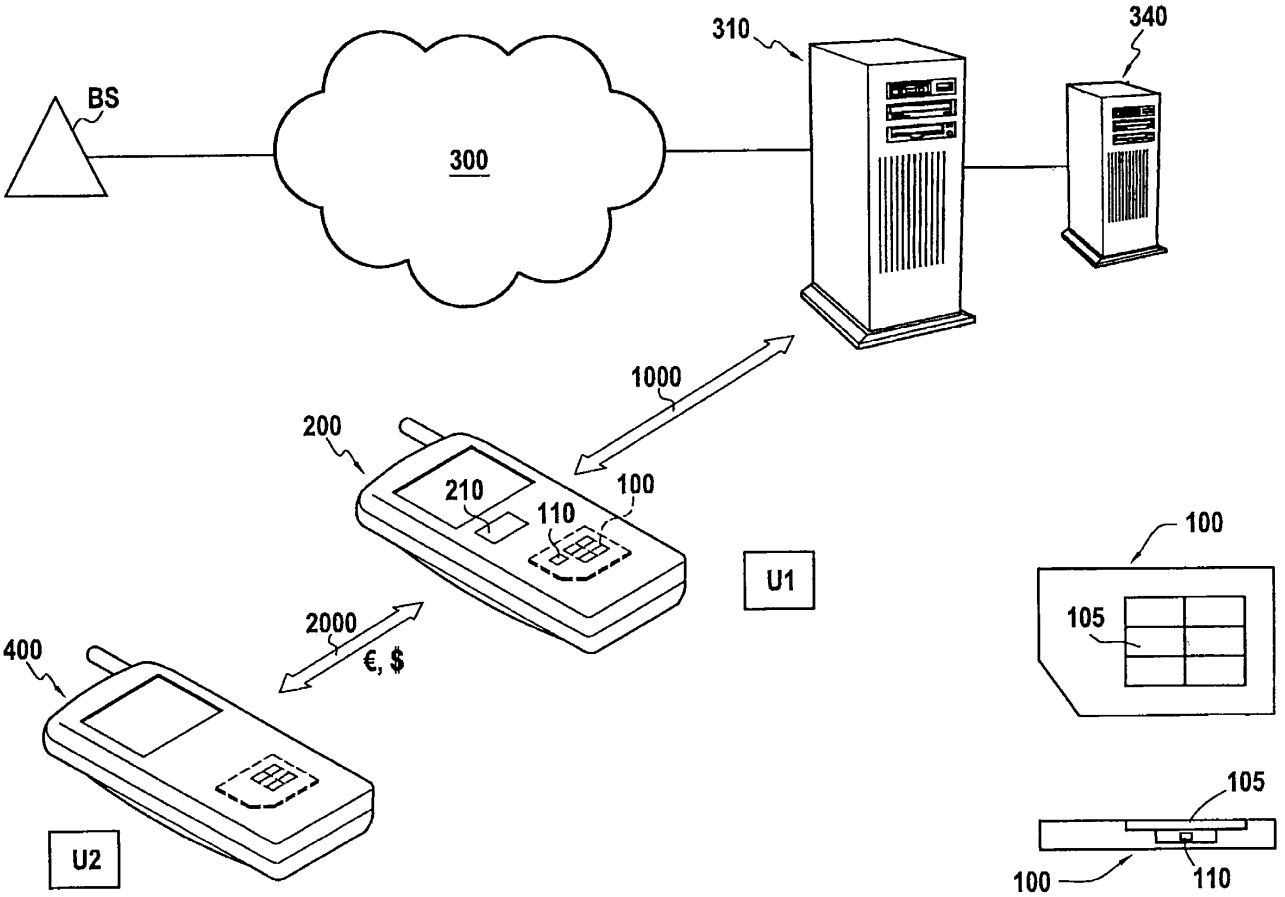
(54) ЗАЩИЩЕННЫЙ ЭЛЕКТРОННЫЙ БЛОК ДЛЯ САНКЦИОНИРОВАНИЯ ТРАНЗАКЦИИ

(57) Реферат:

Изобретение относится к области дистанционных платежей, а именно к платежам в платежном терминале при помощи мобильного электронного устройства. Технический результат – повышение безопасности проведения транзакции. Защищенный электронный блок для проведения транзакции содержит интерфейс связи и средства, которые при установлении связи через указанный интерфейс связи с мобильным электронным устройством, содержащим средства соединения с телекоммуникационной сетью, выполнены с возможностью аутентифицировать удаленный сервер проверки транзакции в телекоммуникационной сети и аутентифицироваться в указанном удаленном сервере, установить защищенное соединение через телекоммуникационную сеть с указанным удаленным сервером, получить через указанный интерфейс связи данные, относящиеся к предполагаемой транзакции с третьим устройством, и передавать данные через защищенное соединение в удаленный сервер для их анализа с целью принятия решения о возможности санкционирования транзакции. 3 н. и 10 з.п. ф-лы, 3 ил.

RU 2651245 C2

RU 2651245 C2



Фиг. 1

RU 2651245 C2

RU 2651245 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 651 245**(13) **C2**

(51) Int. Cl.
G06Q 20/32 (2012.01)
G06Q 20/40 (2012.01)
G06Q 20/38 (2012.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06Q 20/3226 (2006.01); G06Q 20/3829 (2006.01); G06Q 20/40 (2006.01)

(21)(22) Application: **2015104781, 09.07.2013**

(24) Effective date for property rights:
09.07.2013

Registration date:
18.04.2018

Priority:
(30) Convention priority:
13.07.2012 FR 1256779

(43) Application published: **27.08.2016** Bull. № **24**

(45) Date of publication: **18.04.2018** Bull. № **11**

(85) Commencement of national phase: **13.02.2015**

(86) PCT application:
FR 2013/051630 (09.07.2013)

(87) PCT publication:
WO 2014/009646 (16.01.2014)

Mail address:
109012, Moskva, ul. Ilinka, 5/2, OOO "Soyuzpatent"

(72) Inventor(s):
OBEN Yan-Loik (FR),
DYUKROS Kristof (FR),
DEPER Terri (FR),
GOVEN David (FR),
RIKO Ruben (FR)

(73) Proprietor(s):
OBERTUR TEKNOLODZHI (FR)

RU 2651245 C2

RU 2651245 C2

(54) SECURE ELECTRONIC ENTITY FOR AUTHORISING TRANSACTION

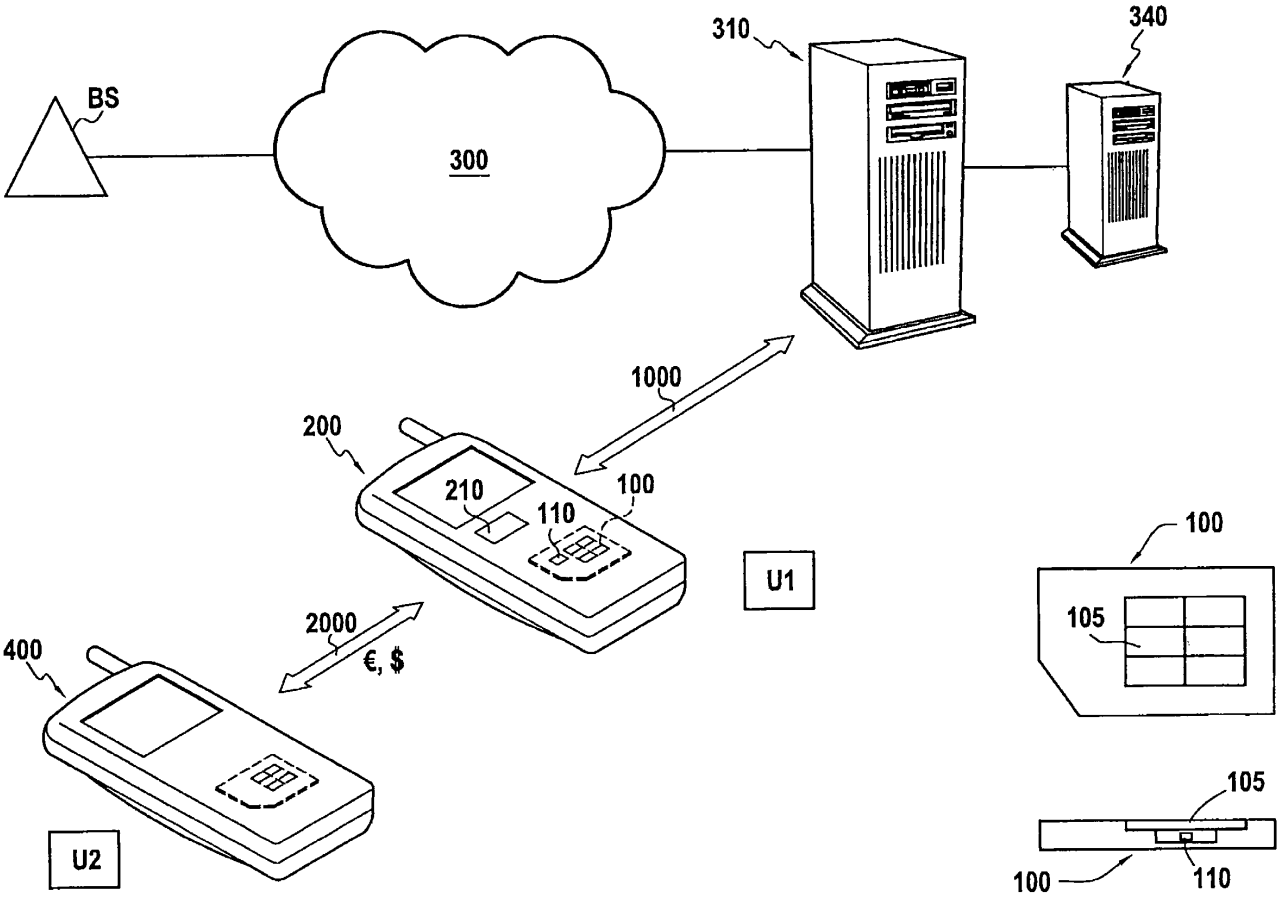
(57) Abstract:

FIELD: data processing; calculation; score.

SUBSTANCE: invention relates to remote payments, specifically payments in a payment terminal using a mobile electronic device. Secure electronic unit for carrying out a transaction comprises a communication interface and means which, when communication is established via said communication interface with a mobile electronic device comprising means for connecting to a telecommunications network, are configured to authenticate a remote transaction verification server in the telecommunications network and authenticate to said remote server, to establish a secure connection through a telecommunications network with said remote server, to receive through said communication interface data relating to the intended transaction with a third device, and transfer data via a secure connection to a remote server for analysis thereof in order to decide whether to authorise the transaction.

EFFECT: technical result is higher security of the transaction.

13 cl, 3 dwg



Фиг. 1

RU 2651245 C2

RU 2651245 C2

Область техники и уровень техники

Изобретение относится к области дистанционных платежей и, в частности, к платежам в платежном терминале при помощи мобильного электронного устройства.

Известно осуществление платежа при помощи карты с микросхемой (банковская смарт-карта) и торгового платежного терминала, соединенного с защищенной коммуникационной сетью, через которую он сообщается с подразделениями платежной системы EMV (Europay Mastercard Visa).

Связь между смарт-картой и платежным терминалом может быть контактной или бесконтактной, в частности, с использованием технологии NFC (Near-Field Communication) (связь в ближнем поле).

Платежный терминал содержит приложение, позволяющее проверять предусматриваемые транзакции с учетом правил, установленных для коммерсанта и платежной карты. В случае необходимости, он запрашивает разрешение от удаленного сервера.

Осуществляющий эти операции платежный терминал является защищенным, и его держатель не может добавлять в него новые приложения.

Таким образом, мобильный телефон или графический планшет не могут быть использованы в качестве платежного терминала без специальных усовершенствований.

В документе WO 2008/063990 описана система для платежа в торговой точке, не обязательно связанной с сетью. Покупатель использует свой мобильный телефон для установления связи с платежным центром через мобильную телефонную сеть. Связь между торговой точкой и мобильным телефоном осуществляется при помощи средства связи короткого радиуса действия или звуковой связи. При этом уровень защиты является низким.

В документе WO 2010/128442 описан платежный терминал, встроенный в защищенную зону карты памяти, такой как флеш-карта памяти, вставляемая в мобильный телефон. Карта содержит вторую защищенную зону, в которую включены одна или несколько платежных карт, выданных одним или несколькими банками пользователю телефона Платежный терминал идентифицирован как принадлежащий банку или учреждению, которое дает его в аренду коммерсанту. Он работает только с инициирующим устройством, которое должен иметь коммерсант. Это решение характеризуется низким уровнем защиты, так как предусматривает наличие платежного терминала в телефоне покупателя.

Чтобы устранить вышеупомянутые недостатки, необходимо разработать защищенное решение для платежа, работающее с существующими совместимыми мобильными телефонами и не требующее от коммерсанта приобретения нового оборудования.

Цель изобретения и его преимущества

В связи с этим предложен защищенный электронный блок, содержащий интерфейс связи, отличающийся тем, что содержит средства, которые при установлении связи через указанный интерфейс связи между ним и мобильным электронным устройством, содержащим средства подключения к телекоммуникационной сети, позволяют:

- аутентифицировать удаленный сервер проверки транзакции в телекоммуникационной сети и аутентифицировать себя перед указанным удаленным сервером,

- затем установить защищенную связь через телекоммуникационную сеть с указанным удаленным сервером,

- получить от мобильного электронного устройства данные, касающиеся предусмотренной транзакции с третьим устройством, и передать их через защищенную связь в удаленный сервер для их анализа с целью принятия решения о возможности

санкционирования транзакции.

Изобретением предложен также сервер проверки транзакции, содержащий соединение с телекоммуникационной сетью, отличающийся тем, что содержит средства для:

- своей аутентификации перед защищенным электронным блоком удаленного электронного устройства в телекоммуникационной сети и аутентификации указанного защищенного электронного блока,

- установления через указанную сеть защищенной связи с указанным защищенным электронным блоком,

- и получения через защищенную связь данных предусмотренной транзакции и обработки этих данных для принятия решения о возможности санкционирования транзакции.

Благодаря этому защищенному электронному блоку и этому серверу проверки транзакции, транзакцию с дистанционным платежом можно производить в условиях защиты. В частности, клиенты пользователя защищенного электронного блока могут осуществлять с ним транзакцию с высоким уровнем доверия, так как они знают, что их данные платежа не будут перехвачены не санкционированным третьим лицом. Кроме того, администратор сервера проверки может санкционировать проверку и подтверждение предусмотренных транзакций, о которых он получает информацию через защищенную связь, так как он знает, что эту информацию могло передать только лицо, располагающее защищенным электронным блоком.

В частном варианте выполнения, чтобы аутентифицировать сервер проверки в телекоммуникационной сети, защищенный электронный блок передает в указанное мобильное электронное устройство первый элемент аутентификации обмена, зашифрованный при помощи секретного ключа защищенного электронного блока, принимает от указанного сервера проверки второй элемент аутентификации обмена, связанный с сервером проверки, и осуществляет сравнение между первым и вторым элементами аутентификации обмена.

В частном варианте выполнения, чтобы аутентифицировать себя перед указанным удаленным сервером, защищенный электронный блок выдает в указанное мобильное электронное устройство параметр идентификации в платежном сервисе, например, номер абонента платежного сервиса, зашифрованный при помощи секретного ключа защищенного электронного блока.

Точно так же, в варианте выполнения, чтобы аутентифицировать защищенный электронный блок, сервер принимает через указанную сеть от удаленного электронного устройства зашифрованную подпись и осуществляет проверку подписи.

Для своей аутентификации перед защищенным электронным блоком сервер может также принимать от удаленного электронного устройства элемент аутентификации обмена, сопровождаемый подписью, производит проверку подписи и в случае положительного результата проверки переправляет указанный элемент аутентификации обмена обратно в защищенный электронный блок.

Предпочтительно электронный блок содержит средства сообщения через указанный интерфейс связи с приложением мобильного электронного устройства при помощи защищенного механизма доступа (типа "Access Control"), что позволяет защищенному электронному блоку передать первый элемент аутентификации обмена, выдать номер абонента или принять данные, касающиеся предусмотренной транзакции, в защищенных условиях. Предпочтительно интерфейс связи может быть выполнен с возможностью установления сообщения между защищенным электронным блоком и интерфейсом связи короткого радиуса действия мобильного электронного устройства. Например,

этот интерфейс связи может быть интерфейсом типа SWP (Single Wire Protocol) (протокол связи по одиночному проводу).

Защищенная связь может быть связью типа SMS (Short Message Service) (служба коротких сообщений), CAT-TP (Card Application Toolkit - Transport Protocol) (инструментарий для карточных приложений - транспортный протокол) или http (Hypertext Transfer Protocol) (протокол передачи гипертекста).

Предпочтительно защищенный электронный блок содержит средства, позволяющие учитывать информацию, принятую от мобильного электронного устройства, указывающую, что удаленный сервер не смог аутентифицировать защищенный электронный блок.

Согласно варианту выполнения, защищенный электронный блок может дополнительно содержать средства для выдачи в указанное мобильное электронное устройство элемента, сохраненного в памяти во время предыдущего использования, чтобы пользователь мобильного электронного устройства мог проверить, что он использует приложение мобильного электронного устройства, которое он уже использовал ранее.

Согласно другому варианту, защищенный электронный блок дополнительно содержит средства для проверки личности пользователя мобильного электронного устройства.

Объектом изобретения является также способ выплаты денежной суммы покупателем коммерсанту, содержащий следующие этапы:

- аутентификация коммерсанта и связанного с коммерсантом мобильного электронного устройства перед удаленным сервером проверки транзакции,
- ввод коммерсантом предназначенной к оплате суммы в связанное с коммерсантом мобильное электронное устройство,
- установление связи короткого радиуса действия между мобильным электронным устройством, связанным с коммерсантом, и мобильным электронным устройством, связанным с покупателем, и выбор среды платежа на мобильном электронном устройстве, связанном с покупателем,
- передача через защищенную связь данных транзакции в удаленный сервер,
- проверка удаленным сервером данных транзакции, чтобы узнать, можно ли санкционировать транзакцию, включая, в частности, этапы управления риском терминала по стандарту EMV.

Преимуществом этого способа является то, что он позволяет использовать мобильное электронное устройство в качестве библиотеки EMV уровня 2 с соответствующими разрешениями, а также позволяет перенести операции проверки в удаленный сервер.

Предпочтительно, но не ограничительно аутентификацию связанного с коммерсантом мобильного электронного устройства перед сервером и установление защищенной связи можно осуществлять при помощи описанного выше защищенного электронного блока.

Краткое описание чертежей

Фиг. 1 - вариант выполнения устройства в соответствии с изобретением.

Фиг. 2 и 3 - вариант осуществления способа в соответствии с изобретением. Описание варианта выполнения.

На фиг. 1 представлены устройства, используемые в изобретении. Коммерсант (кредитор) U1 имеет мобильный телефон 200, содержащий карту SIM (Subscriber Identity Module (модуль идентификации абонента), называемую также UICC, Universal Integrated Circuit Card) (универсальная карта на интегральной схеме 100), выданную коммерсанту,

например, оператором мобильной телефонной связи. Карта SIM 100 показана в увеличенном виде в правой нижней части фиг. 1, вид сверху и вид в разрезе сбоку. Карта SIM 100 имеет интерфейс контактной связи 105, позволяющий ей сообщаться с мобильным телефоном 200, например, типа SWP или IS07816, и включает в себя приложение 110, обычно называемое апплетом, которое конфигурировано организацией, получающей платеж, и в котором записан, в частности, номер абонента организации, получающей платеж. Это приложение ПО позволяет осуществлять транзакцию. Вместо карты SIM можно использовать карту microSD (micro Secure Digital) или встроенный защищенный модуль, называемый eSE.

Мобильный телефон 200 может быть также оснащен платежным приложением продавца 210, обычно называемое MIDLET (то есть соответствующее норме MIDP или "Mobile Information Device Profile") (профиль мобильного информационного устройства), позволяющее ему сообщаться с пользователем (в данном случае коммерсантом U1) для осуществления различных функций терминала торговой точки посредством установления связи с приложением ПО карты SIM 100 и с удаленным сервером (обозначенным 310 и описанным ниже).

Коммерсант вступает в отношения с покупателем (дебитором) U2, который располагает мобильным телефоном 400 или, говоря шире, бесконтактным платежным средством. В случае, если это платежное средство является мобильным телефоном 400, оно имеет платежное приложение покупателя (не показано), которое предварительно было выдано покупателю его банком или, говоря шире, эмитентом платежных средств.

Телефон 200 выполнен с возможностью подключения к мобильной телефонной сети 300 через базовую станцию BS. Телефоны 200 и 400 могут сообщаться друг с другом напрямую при помощи средств беспроводной связи короткого радиуса действия, например, типа NFC, отвечающих норме ISO 14443. Интерфейс связи 105, например, типа SWP, позволяет защищенному электронному блоку сообщаться со средствами беспроводной связи короткого радиуса действия типа NFC терминала.

Сервер 310 связан с мобильной телефонной сетью 300. Карта SIM 100 и сервер 310 выполнены с возможностью установления между собой защищенной связи через базовую станцию мобильной телефонной связи. Сервер 310 является сервером проверки транзакций, управляемый организацией, абонентом которой является коммерсант.

Сервер 310 проверки транзакций может осуществлять связь с вторым сервером 340, который связан с сервером эмитента платежного средства покупателя U2.

Сервер 310 проверки транзакций сообщается по защищенной связи с картой SIM 100.

На фиг. 2 показана первая часть способа платежа в соответствии с изобретением. Коммерсант U1 осуществляет этап E1 активации платежного приложения 201 на своем телефоне 200.

Платежное приложение 210 запускается и выдает на дисплей дату последней акцептированной транзакции, которую оно считывает из карты SIM 100. Это визуальное указание позволяет коммерсанту U1 убедиться, что используемое им приложение является аутентичным приложением, которое не было заменено пиратским (вредоносным или другим) приложением с момента последней транзакции. Можно также использовать и другую динамическую информацию.

Платежное приложение 210 телефона 200 приглашает после этого коммерсанта U1 ввести его код PIN (Personal Identification Number) (личный идентификационный номер) через интерфейс человек-машина в ходе этапа E2 запроса кода PIN. Коммерсант U1 вводит свой код PIN на этапе E3. Можно также использовать другие методы

идентификации коммерсанта, например, такие как распознавание биометрических данных. В варианте активация приложения 210 может также сопровождаться считыванием наружной этикетки (tag), содержащей данные аккредитации коммерсантаU1.

Затем на этапе E4 платежное приложение 210 телефона 200 предлагает через интерфейс человек-машина коммерсанту U1 ввести оплачиваемую сумму. Коммерсант выдает эту информацию платежному приложению телефона 200 на этапе E5.

На этапе E6 платежное приложение 210 телефона 200 выводит на дисплей сообщение приглашения, предназначенное для покупателя U2, предлагающее ему расположить его платежное средство вблизи средств связи короткого радиуса действия телефона 200. На этапе E7 коммерсант U1 устно предлагает покупателю U2 расположить его платежное средство напротив телефона 200.

Параллельно с этапами E4-E7 во время этапа E8 код РПЧ коммерсанта поступает из приложения 210 телефона 200 в приложение ПО карты SIM 100. Приложение 110 является защищенным приложением, которое было загружено в карту SIM 100 с соблюдением связанных с ней критериев защиты. Таким образом, оно является полностью защищенным. Связь между платежным приложением 210 телефона и приложением ПО карты SIM можно осуществлять, например, при помощи механизма Access Control для аутентификации платежного приложения телефона перед картой SIM (этап E8 показан в виде сокращения AC на фиг. 2 для обозначения этой защиты).

В свою очередь, приложение ПО проверяет код PIN (конфиденциальный код коммерсанта), затем в ответ на запрос приложения 210 создает элемент аутентификации обмена, специально выбранный для обмена, который оно должно осуществить с сервером 310. В данном случае этот элемент аутентификации обмена представляет собой случайное число или любой другой тип переменной данной, и его выбирают после проверки кода PIN апплет-приложением или в момент запуска апплет-приложения.

При этом приложение ПО карты SIM 100 создает сообщение, одновременно содержащее случайное число и специальный номер коммерсанта (номер абонента), который был введен в карту SIM 100 в момент ее персонализации. Приложение ПО подписывает и шифрует сообщение, используя ключ асимметричного шифрования, который тоже был введен в карту SIM.

Апплет ПО карты SIM 100 передает зашифрованное сообщение в платежное приложение 210 телефона 200 на этапе E9 (защищен механизмом Access Control). Платежное приложение 210 телефона выполнено с возможностью передачи этого сообщения в сервер 310 на этапе ЕЮ, который является этапом запроса аутентификации карты SIM 100 сервером 310. Эту передачу осуществляют при помощи технологии связи, используемой в сети 300, например, посредством передачи SMS, сообщения USSD (Unstructured Supplementary Service Data) (неструктурированные дополнительные служебные данные) или команды HTTP. Передача для сервера 310 происходит при помощи адреса этого сервера, например номера телефона или Интернет-адреса, который записан в платежном приложении телефона 200 или в карте SIM 100.

Сервер 310 анализирует содержание принятого сообщения, дешифруя его при помощи ключа, соответствующего ключу, ранее использованному приложением ПО. Следует уточнить, что вместо пары асимметричных ключей можно использовать и другие криптографические средства.

Сервер 310 проверяет подпись и номер коммерсанта. Затем, если номер коммерсанта соответствует подписи, он делает вывод, что сообщение было передано именно приложением 110 карты SIM, которая была выдана коммерсанту U2. Терминал 310

передает ответное сообщение в приложение 110 карты SIM 100, например, в виде SMS. На этапе ЕП терминал передает стандартное сообщение PUSH, представляющее собой команду, предназначенную для приложения 110 карты SIM 100, на открытие с ним защищенной связи. Это сообщение содержит случайное число, которое было генерировано картой SIM 100.

Приложение 110 карты SIM 100 принимает сообщение PUSH, дешифрует его и сравнивает содержащееся в нем число и с ранее генерированным им случайным числом. Если они совпадают, приложение делает вывод, что отправитель сообщения PUSH является надлежащим и аутентичным сервером, которым управляет платежное учреждение.

После этого приложение ПО карты SIM генерирует предназначенную для сервера 310 команду, например, Openchannel, как указано в стандарте ETSI TS 102223, на открытие защищенной связи типа SMS, CAT-TP или HTTP (последний вариант определен в документе Приложение B стандарта Global Platform (глобальная платформа)). Передача этой команды происходит на этапе E12.

Например, после этого между приложением ПО карты 100 и сервером 310 создается защищенный канал связи 1000 при помощи команд UDP (User Datagram Protocol (протокол пользовательских дейтаграмм) для канала CAT-TP) или TCP/IP (Transmission Control Protocol/Internet Protocol (протокол управления передачей/интернет-протокол) для канала HTTP), передаваемых телефоном 200 (независимо от платежного приложения), который взаимодействует с картой SIM при помощи команд и квитанций APDU (Application Protocol Data Unit) (блок данных протокола приложения) для активации системы Bearer Independent Protocol (протокол, независимый от носителя) (BIP).

В варианте между сервером 310 и приложением ПО происходит обмен, который является прозрачным для телефона 200.

На этапе E13 сервер 310 передает параметры коммерсантов в приложение ПО через защищенную связь 1000. Параметры коммерсантов включают в себя список AID (идентификаторы банковских приложений для платежного терминала), валюты, потолки и другие данные, позволяющие приложению автономно реализовать платежную транзакцию между коммерсантом U1 и покупателем U2 через телефоны 200 и 400 (что в рамках транзакции EMV включает в себя следующие функции: выбор приложения, Get Processing Option (получить опцию обработки), Read record (считать запись) и Generate AC (генерировать AC)). Преимуществом этапа E13 является возможность использования телефона 200 в качестве библиотеки EMV уровня 2 с соответствующими разрешениями. Обмен параметров коммерсантов между телефоном 200 и картой SIM 100 происходит в условиях защиты при помощи механизма Access Control.

Параллельно с этапами E1-E13 покупатель U2 осуществляет этап F1 активации платежного приложения покупателя телефона 400. Эта активация может включать в себя набор персонального кода и выбор среды платежа.

На фиг. 3 представлено продолжение способа в соответствии с изобретением. Здесь опять показан этап E13 передачи параметров коммерсанта в карту SIM 100 или в платежное приложение телефона 200.

За ним следует этап E14 связи между телефоном 100 и телефоном 200 через их интерфейсы NFC, чтобы телефон 200 мог выбрать ту же платежную среду, которую выбрал телефон 100, чтобы установить опции обработки и чтобы осуществить аутентификацию данных платежного приложения телефона 400 и проверить номер платежного средства (номер PAN, Primary Account Number (первичный номер счета)) и соответствующую дату истечения срока действия, причем эти данные присутствуют в

карте SIM телефона 400 и были выданы покупателю U1 во время его абонирования в банке.

Затем осуществляют этап E15 идентификации покупателя U2 посредством ввода его персонального кода. Можно также использовать другие методы идентификации, в частности биометрическое распознавание. Вместе с тем, для транзакции на небольшую сумму идентификацию покупателя можно не осуществлять. Персональный код вводят при помощи клавиатуры телефона 400 и проверяют посредством установления связи между телефонами 400 и 200.

После этого следует этап E16 управления риском терминала (коммерсанта). Этот этап полностью происходит на сервере 310. Он может включать в себя проверку хронологии транзакций за данный день для коммерсанта U1. Преимуществом этапа E16 является перенос в сервер 310 операций проверки, например, Card Holder verification (проверка держателя карты) и Terminal Risk Management (Управление рисками терминала), обычно осуществляемых в бесконтактном платежном терминале.

Затем осуществляют этап E17 генерирования криптограммы транзакции в базе данных транзакции (сумма, дата, место) и банковских данных (банковский идентификатор пользователя телефона 400). Эта криптограмма является результатом взаимодействия карты SIM телефона 400 и платежного приложения телефона 200.

Во время этапов E14-E17 приложение 110 карты SIM 100 остается не активным.

Затем осуществляют этап E18 передачи данных транзакции из платежного приложения 210 телефона 200 в приложение 110 карты SIM 100 в условиях защиты при помощи механизма Access Control. После этого производят передачу данных, в случае необходимости, подписанных и зашифрованных, через защищенную связь 1000 в сервер 310 санкционирования платежа в ходе этапа E19. Эта передача касается суммы транзакции, номера PAN, даты, места и криптограммы. Сервер 310 проверяет данные транзакции и принимает решение о санкционировании транзакции или о ее отмене. Он может также счесть необходимым запросить разрешение у эмитента платежного средства и в этом случае он связывается с сервером 340 на этапе E20, чтобы получить такое разрешение, которое он получает на этапе E21. Если транзакция санкционирована, осуществляют этап E22, в ходе которого сервер 310 направляет свой ответ через защищенную связь 1000 в карту SIM 100. На этапе E23 сервер 310 направляет в карту SIM 210 квитанцию при помощи SMS. Квитанция указывает на результат транзакции.

Изобретение не ограничивается представленными вариантами выполнения и охватывает все версии, не выходящие за рамки объема формулы изобретения. В частности, вместо мобильной телефонной сети сеть 300 может быть расширенной сетью (например, Интернет), к которой телефон 200 (или сенсорный планшет или другое мобильное электронное устройство) получает доступ через связь Wi-Fi.

(57) Формула изобретения

1. Защищенный электронный блок (100) для проведения транзакции, содержащий интерфейс связи (105), отличающийся тем, что содержит средства, которые при установлении связи через указанный интерфейс связи (105) между защищенным электронным блоком и мобильным электронным устройством (200), содержащим средства подключения к телекоммуникационной сети (300), выполнены с возможностью:

аутентифицировать удаленный сервер (310) проверки транзакции в телекоммуникационной сети (300) и аутентифицироваться в указанном удаленном сервере (310),

устанавливать защищенное соединение (1000) через телекоммуникационную сеть с

указанным удаленным сервером (310),

получать (E18) через указанный интерфейс связи (105) данные, относящиеся к предполагаемой транзакции (2000) с третьим устройством (400), и передать (E19) данные через защищенное соединение (1000) в удаленный сервер (310) для их анализа с целью принятия решения о возможности санкционирования транзакции,

при этом защищенный электронный блок представляет собой защищенный электронный блок мобильного электронного устройства (200), причем защищенный электронный блок является картой модуля идентификации абонента (SIM), микрокартой Secure Digital (microSD) или встроенным защищенным модулем (eSE).

2. Защищенный электронный блок по п. 1, характеризующийся тем, что выполнен с возможностью, для аутентификации сервера (310) проверки в телекоммуникационной сети (300), передачи (E9) через указанный интерфейс связи (105) первого элемента аутентификации обмена, зашифрованного при помощи секретного ключа защищенного электронного блока (100), приема (E11) от указанного сервера (310) проверки второго элемента аутентификации обмена, связанного с сервером проверки, и выполнения сравнения между первым и вторым элементами аутентификации обмена.

3. Защищенный электронный блок по п. 1 или 2, характеризующийся тем, что выполнен с возможностью, для аутентификации в указанном удаленном сервере, передачи (E9) через указанный интерфейс связи (105) параметра идентификации в платежном сервисе, зашифрованного при помощи секретного ключа защищенного электронного блока (100).

4. Защищенный электронный блок по п. 1 или 2, выполненный так, что защищенное соединение (1000) является соединением типа SMS, CAT-TP или HTTP.

5. Защищенный электронный блок по п. 1 или 2, содержащий средства установления связи через указанный интерфейс связи (105) с приложением (210) мобильного электронного устройства при помощи защищенного механизма доступа.

6. Защищенный электронный блок по п. 1 или 2, в котором интерфейс связи (105) выполнен с возможностью установления связи между защищенным электронным блоком и интерфейсом связи короткого радиуса действия мобильного электронного устройства (200).

7. Защищенный электронный блок по п. 1 или 2, содержащий средства для учета информации, принятой от мобильного электронного устройства, указывающей, что удаленный сервер (310) не смог аутентифицировать защищенный электронный блок (100).

8. Защищенный электронный блок по п. 1 или 2, дополнительно содержащий средства для выдачи в указанное мобильное электронное устройство элемента, сохраненного в памяти во время предыдущего использования, чтобы позволить пользователю мобильного электронного устройства проверить, что он использует приложение мобильного электронного устройства, которое он уже использовал ранее.

9. Защищенный электронный блок по п. 1 или 2, дополнительно содержащий средства проверки личности пользователя мобильного электронного устройства.

10. Сервер (310) проверки транзакции, содержащий соединение с телекоммуникационной сетью (100), отличающийся тем, что содержит средства для:

своей аутентификации в защищенном электронном блоке (100) удаленного электронного устройства (200) в телекоммуникационной сети (300) и для аутентификации указанного защищенного электронного блока,

установления через указанную сеть защищенной связи с указанным защищенным электронным блоком (100),

и получения (E19) через защищенную связь(1000) данных предполагаемой транзакции (2000) и обработки указанных данных для принятия решения о возможности санкционирования транзакции,

причем защищенный электронный блок является картой модуля идентификации абонента (SIM), микрокартой Secure Digital (microSD) или встроенным защищенным модулем (eSE).

11. Сервер по п. 10, характеризующийся тем, что выполнен с возможностью для аутентификации защищенного электронного блока (100), принимать (E10) от удаленного электронного устройства (200) через указанную сеть зашифрованную подпись и выполнять проверку подписи.

12. Сервер по п. 10 или 11, характеризующийся тем, что выполнен с возможностью, для аутентификации себя в защищенном электронном блоке (100), принимать (E10) от удаленного электронного устройства (200) элемент аутентификации обмена, сопровождаемый подписью, выполнять проверку подписи и, в случае положительного результата проверки, переправлять (E11) указанный элемент аутентификации обмена в направлении защищенного электронного блока (100).

13. Способ выплаты денежной суммы покупателем (U2) коммерсанту (U1), содержащий этапы, на которых:

аутентифицируют связанное с коммерсантом мобильное электронное устройство в удаленном сервере проверки транзакции при помощи защищенного электронного блока,

вводят при помощи коммерсанта (U1) предназначенную к оплате сумму в связанное с коммерсантом мобильное электронное устройство,

устанавливает связь короткого радиуса действия между мобильным электронным устройством, связанным с коммерсантом, и мобильным электронным устройством, связанным с покупателем, и выбирают (F1) среду платежа на мобильном электронном устройстве, связанном с покупателем,

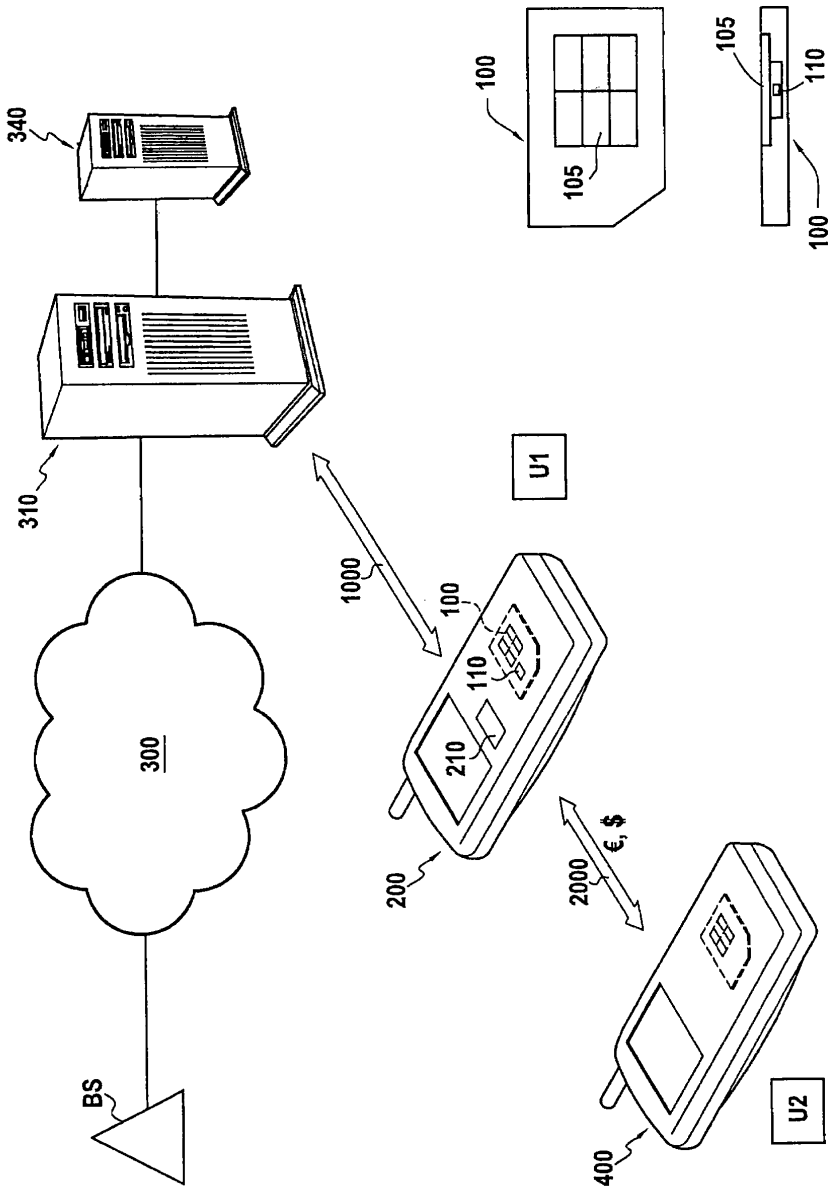
передают данные транзакции в удаленный сервер через защищенное соединение (1000), установленное при помощи защищенного электронного блока,

проверяют на удаленном сервере данные транзакции, чтобы узнать, можно ли санкционировать транзакцию, включая, в частности, этапы (E16) управления риском терминала по стандарту EMV,

при этом защищенный электронный блок представляет собой защищенный электронный блок мобильного электронного устройства (200), причем защищенный электронный блок является картой модуля идентификации абонента (SIM), микрокартой Secure Digital (microSD) или встроенным защищенным модулем (eSE).

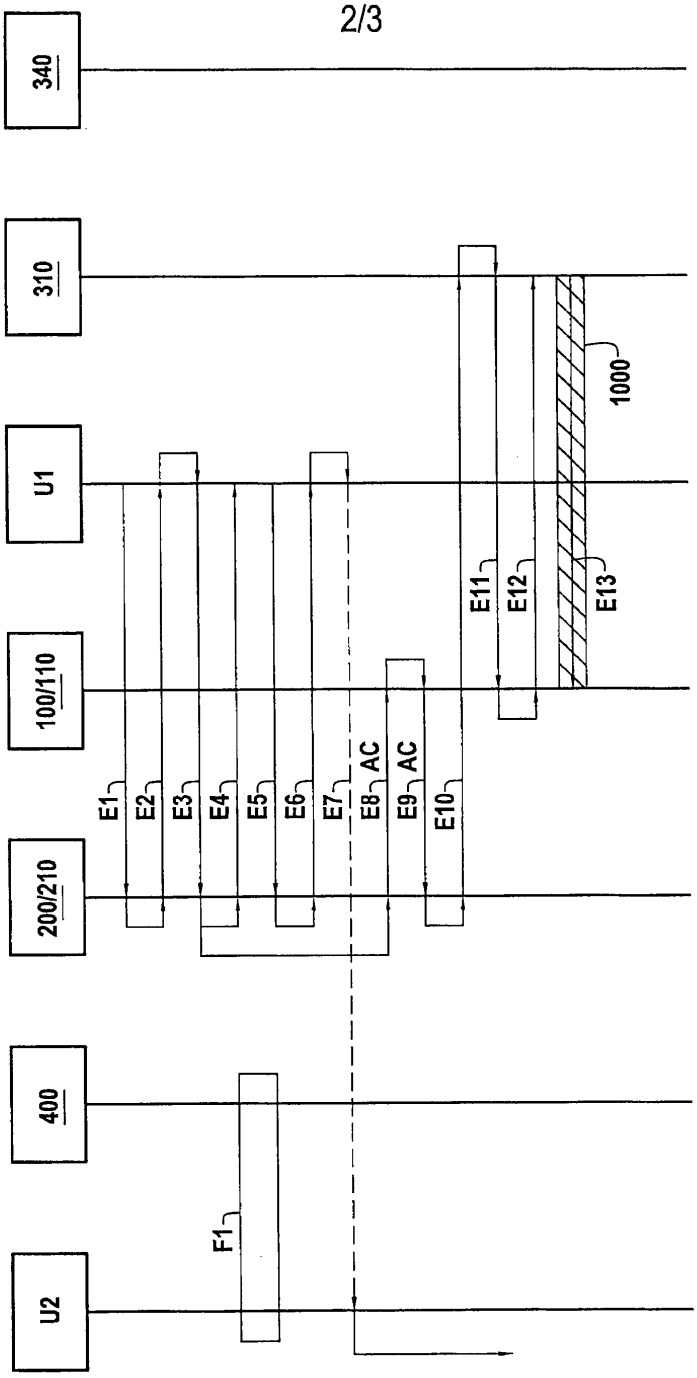
1

1/3


340
310
300
BS
1000
100
110
210
200
U1
2000
€, $
400
U2
100
105
105
110
100

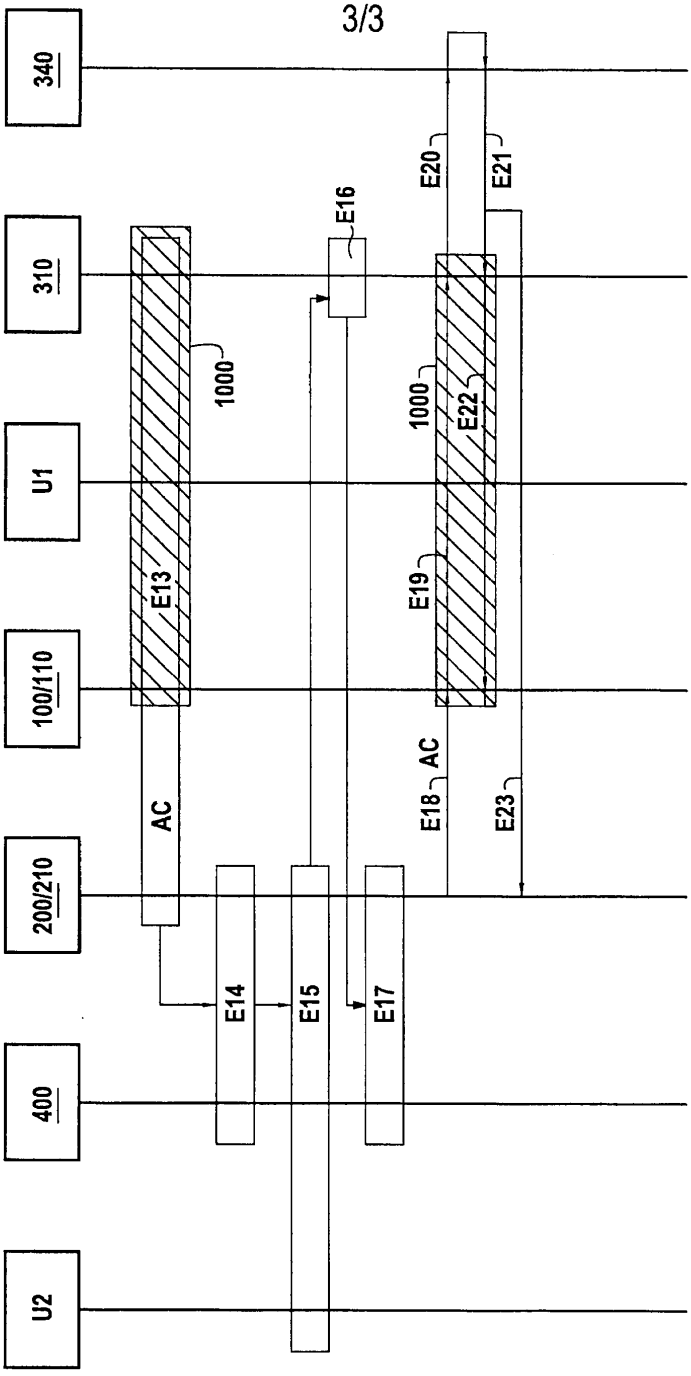
Фиг. 1

2


340
310
U1
100/110
200/210
400
U2
1000
E1
E2
E3
E4
E5
E6
E7
E8
AC
E9
AC
E10
E11
E12
E13
F1

Фиг. 2

3


340
310
U1
100/110
200/210
400
U2
E13
1000
E16
E20
E21
1000
E22
E19
AC
E18
AC
E23
E14
E15
E17

Фиг. 3