РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 576 586**(13) **C2**

(51) МПК
G06Q 20/32 (2012.01)
G06F 21/00 (2013.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2014121883/08, 30.10.2012**

(24) Дата начала отсчета срока действия патента:
30.10.2012

Приоритет(ы):
(30) Конвенционный приоритет:
31.10.2011 EP 11187273.5

(43) Дата публикации заявки: **10.12.2015** Бюл. № **34**

(45) Опубликовано: **10.03.2016** Бюл. № **7**

(56) Список документов, цитированных в отчете о поиске: **WO 2008/052592 A1, 08.05.2008. WO 2010/043722 A1, 22.04.2010. WO 98/25371 A1, 11.06.1998. US 2008/0035725 A1, 14.02.2008. US 2006/0237531 A1, 26.10.2006.**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **02.06.2014**

(86) Заявка PCT:
EP 2012/071472 (30.10.2012)

(87) Публикация заявки PCT:
WO 2013/064493 (10.05.2013)

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

(72) Автор(ы):
АДЕНУГА Доминик (DE)

(73) Патентообладатель(и):
МАНИ ЭНД ДЭЙТА ПРОТЕКШН ЛИЦЕНЦ ГМБХ УНД КО.КГ (DE)

RU 2576586 C2

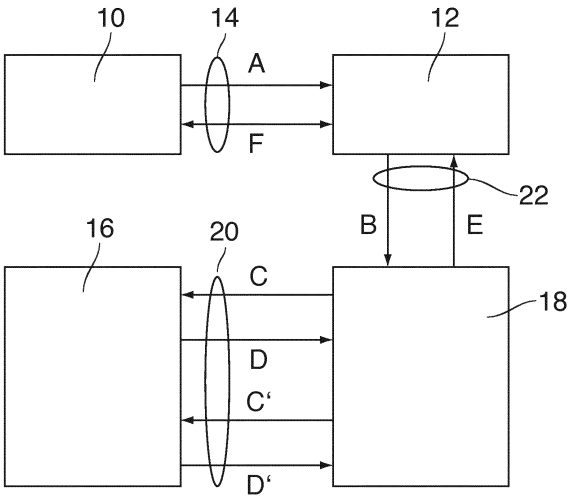
(54) СПОСОБ АУТЕНТИФИКАЦИИ

(57) Реферат:

Изобретение относится к области аутентификации пользователя. Технический результат - эффективная аутентификация пользователя во время транзакций. Способ аутентификации пользователя для транзакции в терминале, в котором идентификатор пользователя передается от терминала партнеру по транзакции через первый канал связи, и используется второй канал связи для проверки функции аутентификации, которая реализована в мобильном устройстве пользователя, функция аутентификации обычно является не активной и активируется пользователем только предварительно по отношению к транзакции, и в качестве критерия для решения, следует ли выдать или отклонить аутентификацию для транзакции, устройство аутентификации проверяет, существует ли заданное временное отношение между передачей идентификатора пользователя и активным состоянием функции аутентификации, причем устройство аутентификации связывается со вторым каналом связи для проверки активного состояния функции аутентификации и принимает ответ от второго канала связи, причем упомянутый ответ включает в себя информацию о том, что функция

аутентификации является активной, и функция аутентификации автоматически деактивируется.

2 н. и 24 з.п. ф-лы, 10 ил.



Фиг. 1

RU 2576586 C2

RU 2576586 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 576 586**(13) **C2**

(51) Int. Cl.
G06Q 20/32 (2012.01)
G06F 21/00 (2013.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2014121883/08, 30.10.2012**

(24) Effective date for property rights:
30.10.2012

Priority:
(30) Convention priority:
31.10.2011 EP 11187273.5

(43) Application published: **10.12.2015** Bull. № **34**

(45) Date of publication: **10.03.2016** Bull. № **7**

(85) Commencement of national phase: **02.06.2014**

(86) PCT application:
EP 2012/071472 (30.10.2012)

(87) PCT publication:
WO 2013/064493 (10.05.2013)

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

(72) Inventor(s):
ADENUGA Dominik (DE)

(73) Proprietor(s):
MANI END DEJTA PROTEKSHN LITSENTS GMBKH UND KO.KG (DE)

RU 2576586 C2

(54) AUTHENTICATION METHOD

(57) Abstract:

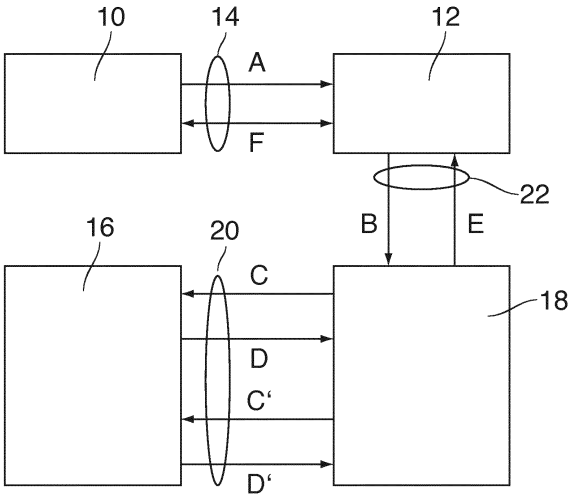
FIELD: information technology.

SUBSTANCE: method of authenticating a user to a transaction at a terminal, wherein a user identifier is transmitted from the terminal to a transaction partner via a first communication channel, and a second communication channel is used for checking an authentication function which is implemented in a mobile device of the user, and the authentication function is normally inactive and is activated by the user only preliminarily for the transaction, and, as a criterion for deciding whether the authentication to the transaction is to be granted or denied, the authentication device checks whether a predetermined time relation exists between the transmission of the user identifier and the active state of the authentication function. The authentication device is linked with the second communication channel to check the active state of the authentication function and receives a response from the second communication channel. Said response includes the information that the authentication function is active, and the authentication function is automatically deactivated.

EFFECT: efficient user authentication during transactions.

26 cl, 10 dwg

RU 2576586 C2



Фиг. 1

RU 2576586 C2

RU 2576586 C2

Изобретение относится к способу аутентификации пользователя для транзакции в терминале, в котором идентификатор пользователя передается от терминала партнеру по транзакции через первый канал связи, и используется второй канал связи для проверки функции аутентификации, которая реализована в мобильном устройстве пользователя, функция аутентификации обычно является не активной и активируется пользователем только предварительно по отношению к транзакции, и в качестве критерия для решения, следует ли выдать или отклонить аутентификацию для транзакции, устройство аутентификации проверяет, существует ли заданное временное отношение между передачей идентификатора пользователя и активным состоянием функции аутентификации.

В транзакциях, в которых пользователь взаимодействует с удаленным партнером по транзакции через канал связи, такой как Интернет, важно гарантировать, что человек, который идентифицирует себя как авторизованный пользователь, фактически является человеком, за которого он себя выдает. Например, когда пользователь делает сетевую банковскую транзакцию, в которой он идентифицирует себя как владелец некоторого счета и делает запрос, чтобы сумма денег была переведена на некоторый другой счет, необходим способ аутентификации, чтобы проверить идентифицирующую информацию запрашивающего. Другие примеры транзакций, в которых должна требоваться аутентификация пользователя, представляют собой транзакции, в которых пользователь запрашивает доступ по сети к базе данных или другим сетевым услугам, которые включают в себя уязвимые данные. Другим примером может быть транзакция для управления дверным замком, который обеспечивает физический доступ к охраняемой территории или комнате.

Публикация GB 2398159 A раскрывает способ аутентификации, в котором функция аутентификации запрашивает у пользователя подтверждение транзакции, и соответствующий сигнал подтверждения отправляется от мобильного устройства устройству аутентификации.

Публикация WO 2008/052592 A1 раскрывает систему кредитных карт, в которой мобильное устройство пользователя используется для активирования и деактивирования кредитной карты. Эта система имеет признаки, указанные в ограничительной части пункта 1 формулы изобретения.

Публикация WO 2007/072001 A1 раскрывает способ аутентификации, в котором устройство аутентификации отвечает на передачу идентификатора пользователя отправкой признака аутентификации терминалу, с которого был выполнен запрос транзакции. Этот признак, например, может быть закодирован в цифровом изображении, которое будет отображено на дисплее терминала. Функция аутентификации в мобильном устройстве выполнена с возможностью съемки этого цифрового изображения и отправки его обратно устройству аутентификации через второй канал связи.

Таким образом, можно подтвердить, что человек, который носит мобильное устройство, например, мобильный телефон, фактически присутствует в местоположении терминала, с которого был выполнен запрос транзакции. Таким образом, пока пользователь управляет своим мобильным устройством, способ аутентификации гарантирует, что никакая третья сторона не может фальсифицировать идентифицирующие данные этого пользователя и выполнить какие-либо транзакции на его месте.

Задача настоящего изобретения состоит в создании способа аутентификации, который является удобным в обращении, и который может быть выполнен с мобильными устройствами низкой сложности.

Для решения этой задачи способ аутентификации в соответствии с изобретением отличается тем, что устройство аутентификации связывается со вторым каналом связи для проверки активного состояния функции аутентификации и принимает ответ от второго канала связи, причем упомянутый ответ включает в себя информацию о том, что функция аутентификации является активной, и функция аутентификации автоматически деактивируется.

В этом способе сложность функции аутентификации может быть значительно уменьшена. В крайнем случае все, что должно требоваться от функции аутентификации - это разрешить устройству аутентификации обнаруживать, является ли эта функция активной. Аналогичным образом, единственное действие, которое требуется от пользователя в целях аутентификации, состоит в активировании функции аутентификации при подходящей синхронизации для транзакции. Как только активное состояние функции аутентификации было обнаружено, эта функция возвращается в неактивное состояние. «Заданное временное отношение» может подразумевать, что функция аутентификации является активной в момент, когда идентификатор пользователя отправляют от терминала. В качестве альтернативы, заданное временное отношение может подразумевать, что функция аутентификации активирована в пределах некоторого (предпочтительно короткого) временного окна после передачи идентификатора пользователя, или наоборот, что идентификатор пользователя передается в пределах заданного временного окна после того, как устройство аутентификации обнаружило, что функция аутентификации является активной.

Поскольку функция аутентификации обычно является не активной, аутентификация почти наверняка не сработает, когда третья сторона мошенническим образом идентифицирует себя как пользователь, чтобы инициировать транзакцию. Тогда аутентификация будет успешна только при очень маловероятном событии, что истинный пользователь активирует функцию аутентификации своего мобильного устройства только в нужный момент. Даже в этом маловероятном случае мошенничество может быть обнаружено, поскольку пользователь активирует функцию аутентификации только тогда, когда он сам хочет сделать транзакцию. Следовательно, устройство аутентификации обнаружило бы совпадение между одной активацией функции аутентификации и двумя запросами транзакции (обычно запускаемыми с разных терминалов), и это заставит устройство аутентификации (или партнеров по транзакции) отклонять или возвращать транзакции. Таким образом, несмотря на низкую сложность, способ в соответствии с изобретением предлагает высокий уровень безопасности.

Более конкретные факультативные признаки изобретения указаны в зависимых пунктах формулы изобретения.

Терминал, от которого передается идентификатор пользователя, может представлять собой, например, банковскую машину или кассу, но также может являться любым другим устройством, таким как компьютер, способный к взаимодействию с удаленным партнером по транзакции. Мобильное устройство, например, может являться мобильным телефоном или смартфоном, ноутбуком, планшетным компьютером и т.п., но также может представлять собой специализированное устройство, которое специально разработано с целью описанного здесь способа аутентификации.

Конкретным преимуществом изобретения является то, что мобильное устройство не должно иметь никаких специальных аппаратных средств для получения или вывода информации. Все, что требуется от мобильного устройства - чтобы оно могло быть активировано на некоторый (предпочтительно короткий) промежуток времени и было способно к соединению с сетью мобильной связи, в которой у него есть адрес,

привязанный к идентифицирующим данным пользователя, с тем чтобы устройство аутентификации, когда оно принимает идентификатор пользователя от терминала, было способно проверить, является ли функция аутентификации мобильного устройства с соответствующим адресом активной. С этой целью, даже не является необходимым, чтобы имелась какая-либо фактическая связь между устройством аутентификации и мобильным устройством. Например, когда мобильное устройство имеет приемопередатчик мобильной телефонной связи (GSM), активирование функции аутентификации может состоять только из активирования этого приемопередатчика, с тем чтобы он соединился с ближайшей подсистемой базовой станции (BSS) сети мобильной связи. В результате мобильное устройство будет идентифицировано посредством его идентификатора устройства (IMSI), и информация об активном состоянии мобильного устройства и о соте GSM, в которой оно расположено, будет введена в реестр собственных абонентов (HLR) сети мобильной связи. Таким образом, устройство аутентификации может проверить активное или неактивное состояние мобильного устройства только посредством запроса реестра HLR.

Мобильное устройство может иметь множество адресов мобильной связи (например, номеров мобильных телефонов) и даже может быть способным к взаимодействию через множество разных сетей мобильной связи. В этом случае предпочтительно, чтобы каждый адрес мобильной связи был присвоен своему отдельному типу транзакции (например, один телефонный номер для аутентификации банковской транзакции и другой для аутентификации доступа к сети передачи данных), и функция аутентификации или множество функций аутентификации выполнены с возможностью активирования и деактивирования отдельно для каждого типа транзакции.

В измененном варианте осуществления для улучшенной безопасности множество адресов мобильной связи может быть присвоено одному и тому же типу транзакции, и мобильное устройство и устройство аутентификации используют идентичные алгоритмы для того, чтобы время от времени изменять адрес мобильной связи, который должен использоваться в целях аутентификации.

В качестве дополнительного средства защиты способ в соответствии с изобретением может содержать этап определения местоположения мобильного устройства и проверки в дополнение к заданному временному отношению, имеется ли также заданное пространственное отношение между мобильным устройством и терминалом. В примере, который был описан в предыдущем абзаце, может быть проверено, расположено ли мобильное устройство в соте GSM, которая также содержит местоположение терминала.

Фактически может быть выгодно, когда вообще нет никакого взаимодействия между мобильным устройством и устройством аутентификации, а также между мобильным устройством и терминалом или каким-либо другим объектом, поскольку, когда нет никакого взаимодействия, нет никакой возможности прослушать и использовать это взаимодействие для обхода системы обеспечения безопасности.

В других вариантах осуществления изобретения возможно, что функция аутентификации в мобильном устройстве принимает данные аутентификации от устройства аутентификации через первый или второй канал связи, факультативно обрабатывает эти данные и отвечает устройству аутентификации заданным образом. Например, некоторые детали запроса транзакции, например, номер счета и сумма дебетования в случае банковской транзакции, могут быть переданы от устройства аутентификации мобильному устройству и могут быть показаны пользователю, например, через дисплей устройства. Тогда пользователь может либо подтвердить, либо отклонить запрос. Предпочтительно детали запроса аутентификации отправляют

только после того, как устройство аутентификации подтвердило, что функция аутентификации в мобильном устройстве является активной. Таким образом, если пользователь не активировал функцию аутентификации, не будет никакого дальнейшего взаимодействия через второй канал связи, и пользователь может сэкономить на затратах связи. Если функция аутентификации является активной, взаимодействие через второй канал связи также может включать в себя запрос некоторых деталей аутентификации, например, если операционный терминал является компьютером пользователя, детали аутентификации могут включать в себя IP-адрес компьютера, наличие некоторых файлов данных или конфигураций программного обеспечения на компьютере, местоположении компьютера и т.п. Посредством запроса у пользователя подтвердить или указать такую информацию, которая будет доступна только пользователю, вероятность мошенничества может быть значительно уменьшена. Аналогичным образом возможно, что мобильное устройство отправляет идентифицирующие данные, такие как PIN-код, закодированный отпечаток пальца или рисунок радужной оболочки и т.п. пользователя, разрешая устройству аутентификации проверить, что зарегистрированный пользователь фактически управляет мобильным устройством. Эти процедуры могут гарантировать, что мобильное устройство действительно является устройством, которое идентифицировано посредством идентификатора IMSI, то есть идентификатор IMSI не имитирован.

В соответствии с независимым аспектом изобретения, который однако может быть включено в описанный выше способ, мобильное устройство включает в себя интерфейс для некоторого идентифицирующего признака пользователя. Например, интерфейс может быть устройством считывания карт для считывания смарт-карты с удостоверением личности пользователя. Традиционно устройство считывания для таких смарт-карт или другого идентифицирующего признака соединено с компьютером или терминалом, через который запрашивается транзакция, чтобы сертифицировать идентичность пользователя. Однако эта процедура не устраняет риск того, что компьютер был заражен некоторым шпионским программным обеспечением, с помощью которого могут быть перехвачены данные от смарт-карты. В соответствии с изобретением уязвимые данные от идентифицирующего признака передаются не через компьютер, а через мобильное устройство, которое не может быть заражено или очень маловероятно может быть заражено шпионским программным обеспечением. Факультативно от пользователя может потребоваться активировать идентифицирующий признак, например, посредством ввода пароля.

Когда мобильное устройство представляет собой специализированное устройство, предпочтительно, чтобы электронные компоненты устройства были защищены и от электронного, и от механического доступа.

Варианты осуществления изобретения теперь будут описаны в связи с чертежами.

Фиг. 1 - блок-схема, иллюстрирующая способ аутентификации в соответствии с изобретением;

Фиг. 2-4 - временные диаграммы, иллюстрирующие разные варианты осуществления изобретения;

Фиг. 5 - блок-схема, иллюстрирующая другой вариант осуществления изобретения;

Фиг. 6 - блок-схема, иллюстрирующая пример схемы связи варианта осуществления изобретения;

Фиг. 7 - вид специализированного мобильного устройства для выполнения способа в соответствии с изобретением;

Фиг. 8 - вид в разрезе устройства, показанного на Фиг. 7;

Фиг. 9 - вид специализированного мобильного устройства в соответствии с модифицированным вариантом осуществления;

Фиг. 10 - блок-схема, иллюстрирующая модифицированную схему связи.

Как показано на Фиг. 1, операционный терминал 10, например, банковская машина, взаимодействует с удаленным партнером 12 по транзакции, например, банком, через первый канал 14 связи, который может являться проводным или беспроводным каналом. Мобильное устройство 16 взаимодействует с устройством 18 аутентификации через второй канал 20 связи, который предпочтительно включает в себя беспроводную линию связи, например, сеть мобильной телефонной связи. Устройство 18 аутентификации может быть установлено в помещении партнера 12 по транзакции или может быть выполнено как отдельный объект, взаимодействующий с партнером 12 по транзакции через третий канал 22 связи.

Мобильное устройство 16 носит пользователь, который зарегистрирован как подписчик в сети мобильной телефонной связи, формирующей канал 20 связи. Устройство 18 аутентификации сформировано посредством аппаратного и программного обеспечения для обработки данных и включает в себя базу данных, которая хранит идентификатор (ID) пользователя и номер мобильного телефона (или любой другой адрес мобильной связи) мобильного устройства 16 этого пользователя.

Теперь следует предположить, что пользователь хочет сделать банковскую транзакцию через терминал 10. С этой целью пользователь управляет терминалом 10 и отправляет запрос транзакции партнеру 12 по транзакции. Этот запрос включает в себя этап A передачи идентификатора пользователя партнеру 12 по транзакции. На этапе B партнер 12 по транзакции перенаправляет идентификатор пользователя устройству 18 аутентификации. Вслед за этим устройство 18 аутентификации извлекает номер мобильного телефона и/или международный идентификатор абонента мобильной связи (IMSI) пользователя и связывается с мобильным устройством 16 или по меньшей мере с сетью мобильной телефонной связи, чтобы проверить, является ли активным мобильное устройство 16, или является ли активной некоторая функция аутентификации, реализованная в нем (этап C). Когда на этапе D подтверждено, что функция аутентификации является активной, устройство 18 аутентификации отправляет сигнал аутентификации партнеру 12 по транзакции (этап E). Сигнал аутентификации предпочтительно включает в себя идентификатор пользователя, который был отправлен на этапе B, и сообщает партнеру по транзакции, что этот конкретный пользователь аутентифицирован для запрашиваемой транзакции. Вслед за этим транзакция между пользователем и партнером 12 по транзакции будет выполнена через терминал 10 (этап F).

Факультативно дополнительные этапы C′ и D′ могут быть вставлены между этапами D и E, что также проиллюстрировано на Фиг. 1. Этап C′ будет выполняться только тогда, когда на этапе D было успешно подтверждено, что функция аутентификации является активной, и этап C′ состоит в запросе у пользователя ввести некоторую информацию в мобильное устройство. Например, когда операционный терминал 10 является компьютером, пользователя можно попросить ввести версию программы сканирования вирусов, которая установлена на этом компьютере. Эта информация затем будет передана устройству 18 аутентификации на этапе D′ и будет проверена на соответствие условиям аутентификации, которые были сохранены в нем. Затем сигнал аутентификации (этап E) будет отправлен, только если информация, переданная на этапе D′, включает в себя корректное условие (условия) аутентификации.

Фиг. 2 показывает временную диаграмму, иллюстрирующую один вариант

осуществления способа аутентификации, который был описан в общих чертах выше.

В момент t1 пользователь, который хочет запросить транзакцию, активирует свое мобильное устройство 16. В момент t2 выполняется последовательность этапов A-B-C-D-E, чтобы аутентифицировать пользователя. Поскольку в это время мобильное устройство 16 является фактически активным, аутентификация успешна. Затем в момент t3 мобильное устройство 16 деактивируется либо вручную, либо автоматически посредством функции самостоятельной деактивации, реализованной в устройстве 16. В качестве другой альтернативы команду деактивировать мобильное устройство 16 может отправить устройство 18 аутентификации, когда пользователь был успешно аутентифицирован.

Предпочтительно временной интервал от момента t1 до момента t3, в котором мобильное устройство 16 является активным, будет относительно маленьким, например, составлять только несколько минут или секунд. Когда на этапах C и D обнаружено, что мобильное устройство 16 (или по меньшей мере его функция аутентификации) не является активным, нужно предположить, что человек, который идентифицирован посредством идентификатора пользователя и управляет мобильным устройством 16, фактически не хочет запрашивать транзакцию, и поэтому нужно прийти к заключению, что идентификатор пользователя, отправленный на этапе A, был фальсифицирован несанкционированной третьей стороной. В этом случае аутентификация отклоняется на этапе E.

Фиг. 3 является временной диаграммой для модифицированного процесса аутентификации. В этом варианте осуществления этапы A, B и C, то есть передача идентификатора пользователя и запрос, является ли мобильное устройство 16 активным, выполняется в момент t1′. Вслед за этим устройство 18 аутентификации запускает таймер, который отсчитывает временное окно 24, в пределах которого мобильное устройство 16 должно быть активировано. В показанном примере временное окно 24 начинается в момент t1′ и заканчивается в момент t′3. В других вариантах осуществления временное окно 24 может открываться несколько позже момента t1′. В момент t2′ пользователь активирует мобильное устройство 16, и в ответ на это выполняются этапы D и E. Поскольку момент t2′ находится в пределах временного окна 24, аутентификация является успешной. Если момент t2′ не быть включен во временное окно 24, то аутентификация будет отклонена. Мобильное устройство 16 снова деактивируется в момент t4′.

В другом варианте осуществления, показанном на Фиг. 4, устройство 18 аутентификации проверяет статус функции аутентификации в регулярных временных интервалах (в моменты tc). Процесс аутентификации начинается с активации пользователем мобильного устройства 16 в момент t1″. Более определенно, пользователь активирует функцию аутентификации в устройстве 16. При следующей проверке статуса устройство 18 аутентификации обнаруживает, что функция аутентификации является активной (этап D). Устройство 18 аутентификации реагирует запуском счетчика, который отсчитывает временное окно 26, в пределах которого должен быть передан идентификатор пользователя для успешной аутентификации. В показанном примере пользователь передает свой идентификатор через терминал 10 в момент t2″, который находится во временном окне 26. Поскольку устройство 18 аутентификации уже информировано, что функция аутентификации в устройстве 16 является активной, за этапом B сразу следует этап E, сигнализирующий об успешной аутентификации партнеру 12 по транзакции. Временное окно 26 закрывается в момент t3″. Если этап A был выполнен позже момента t3″, то аутентификация будет отклонена.

Во всех этих вариантах осуществления процесс аутентификации может факультативно включать в себя дополнительные этапы взаимодействия между терминалом 10 и устройством 18 аутентификации и/или между мобильным устройством 16 и устройством 18 аутентификации или в ином случае между терминалом 10 и мобильным устройством 16 (либо непосредственно, либо через пользователя). Такие протоколы связи в целях аутентификации являются хорошо известными в области техники.

Например, мобильное устройство может использовать предварительно запрограммированный алгоритм, чтобы сформировать идентификационный код и отправить его устройству аутентификации. Предварительно запрограммированный алгоритм известен устройству аутентификации и используется в нем для проверки идентифицирующей информации мобильного устройства, независимо от его идентификатора IMSI. Идентификационный код, например, может представлять собой число из списка чисел "TAN", который сохранен в мобильном устройстве, и алгоритм выполнен таким образом, что каждое число используется только один раз. С другой стороны, чтобы разрешить бесконечное количество транзакций, идентификационные коды могут формироваться динамически, возможно с использованием таких данных, как текущая дата или время дня. В еще одном варианте осуществления идентификационный код может представлять собой зашифрованный пароль или зашифрованную комбинацию пароля с данными времени и даты, шифрование основано на динамически меняющемся параметре шифрования, который отправляют от устройства аутентификации.

Аутентификация будет успешна только тогда, когда устройство аутентификации обнаружит, что идентификационный код является допустимым. Однако в любом случае в соответствии с изобретением аутентификация будет отклонена всякий раз, когда обнаружено, что функция аутентификации мобильного устройства 16 не является активной в нужный момент времени.

Фиг. 5 показывает блок-схему, подобную показанной на Фиг. 1, для варианта осуществления, в котором терминал 10 и мобильное устройство 16 физически интегрированы в одном устройстве 30, например, в смартфоне, который имеет доступ к Интернету через сеть мобильной телефонной связи. Таким образом, в этом случае одна часть первого канала 14 связи сформирована сетью мобильной телефонной связи, и другая часть - посредством Интернета, тогда как второй канал 20 связи сформирован только сетью мобильной телефонной связи.

Процедура аутентификации в основном является такой же, как на Фиг. 1-4. Однако, поскольку устройство 30 является многоцелевым устройством, было бы не практично, если бы это устройство в целом было неактивно и активировалось только в течение коротких временных интервалов, когда будет необходима аутентификация. Однако функция аутентификации, которая реализована в мобильном устройстве 16, может принять вид апплета, который может быть активирован и деактивирован независимо от устройства 30 в целом. Тогда, безусловно, на этапе C на Фиг. 5 активное или неактивное состояние функции аутентификации не может быть проверено только посредством запроса сети мобильной телефонной связи, зарегистрировано ли устройство 30 как активное. Вместо этого необходимо, чтобы устройство 18 аутентификации фактически отправило запрос апплету в мобильном устройстве 16, и апплет ответил на этот запрос, когда он активен, или чтобы апплет, когда он активен, отправил запрос устройству аутентификации.

Фиг. 6 иллюстрирует схему связи, в которой первый канал 14 связи и третий канал 22 связи сформированы, например, посредством Интернета. Устройство 18

аутентификации установлено удаленно от партнера 12 по транзакции, и его работа выполняется посредством доверенной третьей стороны, которая независима от партнера 12 по транзакции. Второй канал 20 связи сформирован сетью мобильной телефонной связи, включающей в себя реестр 32 собственных абонентов (HLR) и множество подсистем 34 базовой станции (BSS), из которых только одна показана на Фиг. 6, и каждая из которых служит в качестве одной или нескольких сот 36 мобильной телефонной связи.

В этом варианте осуществления устройство 18 аутентификации не только проверяет, является ли мобильное устройство 16 активным или неактивным, но также идентифицирует соту 36 мобильной связи, в которой в настоящий момент расположено устройство 16, и пользователь аутентифицируется для транзакции только тогда, когда обнаружено, что мобильное устройство 16 является активным в предписанном временном окне и расположено в соте 36, в которой также размещен терминал 10, с которого выполнен запрос транзакции. Таким образом, ложная аутентификация возможна только тогда, когда идентификатор пользователя отправляют с некоторого терминала 10 в нужный момент времени, и кроме того мобильное устройство 16 истинного пользователя оказывается расположенным вблизи этого терминала 10.

Если сеть 20 мобильной связи поддерживает услуги на основе местоположения (LBS), то текущее местоположение мобильного устройства 16 может быть идентифицировано с намного более высоким пространственным разрешением, и успешная аутентификация может потребовать, чтобы мобильное устройство 16 находилось лишь в нескольких сотнях или нескольких десятках метров от терминала 10.

В еще одном варианте осуществления мобильное устройство 16 может включать в себя функцию глобальной системы позиционирования (GPS), и функция аутентификации может быть выполнена с возможностью отправки текущих координат GPS мобильного устройства 16 устройству 18 аутентификации.

Изобретение также включает в себя вариант описанного выше способа, в котором сначала проверяются пространственные отношения между мобильным устройством и терминалом, а временное отношение между передачей идентификатора пользователя и активацией мобильного устройства проверяется только в случае, если это пространственные отношения не выполнено. Например, мобильное устройство может иметь функцию автоматического соединения с сетью мобильной связи в некоторых интервалах, например, несколько раз в день. Затем, когда запрос аутентификации передается вместе с идентификатором пользователя, устройство 18 аутентификации может определить местоположение мобильного устройства 16 посредством обращения к реестру HLR сети мобильной связи, и когда обнаружено, что мобильное устройство находится близко к терминалу или по меньшей мере расположено в «безопасной» области, то есть в области, где вероятность мошенничества является маленькой, например. когда мобильное устройство расположено в некоторой стране или штате, аутентификация выдается без проверки активного состояния функции аутентификации. Таким образом, пользователь не должен активировать функцию аутентификации. С другой стороны, когда обнаружено, что мобильное устройство расположено за рубежом, где вероятность мошенничества выше, аутентификация будет отклонена, если пользователь не активирует функцию аутентификации с корректной синхронизацией.

Этот вариант способа обеспечивает повышенный уровень безопасности с учетом так называемых ловушек IMSI, то есть устройств, которые прослушивают взаимодействия мобильного устройства, чтобы собрать некоторую информацию об мобильном устройстве, например, его идентификатор IMSI. Такие ловушки IMSI

эффективны только тогда, когда мобильное устройство соединяется с сетью мобильной связи, в то время как оно расположено в непосредственной близости от ловушки IMSI, например, на расстоянии менее 1 км. Следовательно, когда ловушка IMSI установлена около терминала, чтобы отловить идентификаторы IMSI пользователей, которые делают транзакции в этом терминале, и терминал расположен в «безопасной» области, где временное отношение не проверяется, ловушка IMSI не сработает, поскольку устройство аутентификации может определить местоположение мобильного устройства уже посредством обращения к реестру HLR, и у мобильного устройства нет необходимости соединяться с сетью мобильной связи, в то время как пользователь расположен близко к терминалу и, следовательно, в пределах досягаемости ловушки IMSI.

Способы аутентификации, использующие дополнительный критерий местоположения, обеспечивают увеличенный уровень безопасности, но имеют проблему, заключающуюся в том, что технически партнер 12 по транзакции может быть способен постоянно отслеживать мобильное устройство 16, вследствие чего могут быть нарушены требования или законы относительно конфиденциальности. Однако конфиденциальность пользователей может быть сохранена посредством гарантии, что адреса мобильной связи, идентификаторы IMSI или телефонные номера мобильных устройств 16 известны только доверенной третьей стороне, выполняющей работу устройства 18 аутентификации, но не партнеру 12 по транзакции. Тогда устройство 18 аутентификации будет уведомлять партнера 12 по транзакции только о том, аутентифицирован ли пользователь, но не будет раскрывать текущее местоположение пользователя. Поскольку партнер по транзакции не имеет доступа к идентификатору IMSI мобильного устройства пользователя, эта процедура также устраняет риск того, что нечестный партнер по транзакции имитирует идентификатор IMSI и/или раскрывает какие-либо другие уязвимые данные пользователя.

Как показано на Фиг. 6, устройство 18 аутентификации может обеспечить анонимизированные службы аутентификации для множества партнеров 12a, 12b по транзакции, например, для множества банков, Интернет-провайдеров и т.п. Используемые способы аутентификации могут отличаться для разных партнеров по транзакции и также могут включать в себя способы типа, проиллюстрированного на Фиг. 1-5, которые используют только временной критерий.

Фиг. 7 и 8 показывают пример мобильного устройства 16, которое является специализированным для конкретной цели аутентификации в соответствии с изобретением. Это устройство 16 имеет корпус 38, который вмещает беспроводной приемопередатчик 40 (например, приемопередатчик мобильной телефонной связи) с антенной 42, электронный контроллер 44, аккумулятор 46 и сигнальную лампу 47 заряда аккумулятора.

Идентификатор устройства (IMSI) постоянно хранится в контроллере 44, который имеет единственную функцию, состоящую в активировании и деактивировании приемопередатчика 40, с тем чтобы последний мог соединяться с ближайшей системой 34 BSS и идентифицировать себя в ней. Переключатель 48 сформирован на поверхности корпуса 38. Переключатель 48 может быть сформирован просто посредством кнопки, с тем чтобы пользователь мог активировать функцию аутентификации (то есть приемопередатчик 40) посредством нажатия кнопки. В качестве альтернативы, переключатель может быть сформирован посредством устройства ввода для ввода некоторого секретного кода (например, PIN-кода) или биометрического датчика, такого как датчик отпечатка пальца или датчик распознавания радужной оболочки, вследствие

чего приемопередатчик будет активирован только тогда, когда подтверждена идентифицирующая информация пользователя. Как показано на Фиг. 9, обеспечен зуммер 49 для выдачи акустической обратной связи, когда функция аутентификации была успешно активирована посредством нажатия переключателя 48.

Контроллер 44 имеет функцию самостоятельной деактивации, которая деактивирует приемопередатчик 40 спустя несколько секунд после того, как он был активирован.

Корпус 38 имеет относительно малые размеры и присоединен к брелоку 50 для ключей, с тем чтобы его можно было удобно носить на связке ключей пользователя.

От одного конца корпуса 38 выступает штепсельный разъем 52 (например, разъем USB или разъем микро-USB), который соединен с аккумулятором 46, с тем чтобы аккумулятор мог быть заряжен посредством подключения устройства 16 в гнездовой разъем USB компьютера, мобильного телефона и т.п. Штепсельный разъем 52 закрыт и защищен съемной крышкой 54. В показанном примере крышка 54 образует гнездовой разъем 56, который открыт с внешней стороны и внутренне соединен с другим гнездовым разъемом 58, в который помещен штепсельный разъем 52. Таким образом, аккумулятор 46 также может быть заряжен посредством подключения штепсельного разъема USB или микро-USB источника питания в разъем 56.

Как показано на Фиг. 8, корпус 38 представляет собой массивный пластмассовый корпус с залитыми в него приемопередатчиком 40, контроллером 44 и аккумулятором батарея 46. Таким образом, физический доступ к этим компонентам, особенно к приемопередатчику 40 и контроллеру 44, не возможен без разрушения корпуса 38.

В модифицированном варианте осуществления контроллер 44 может включать в себя запоминающее устройство с программным кодом и данными для более сложных функций аутентификации, например, для функции формирования и передачи идентификационного кода устройства, как было описано выше. Однако контроллер не имеет каких-либо электронных контактов, которые обеспечили бы возможность для считывания содержания запоминающего устройства. Факультативно контроллер 44, и особенно его запоминающее устройство, может быть выполнен таким образом, что все сохраненное содержание стирается, как только корпус 38 ломается, и кто-либо пытается удалить из него контроллер. Таким образом, данные аутентификации, которые могут быть сохранены в запоминающем устройстве контроллера 44, надежно защищены от копирования.

Фиг. 9 показывает пример мобильного устройства 16′, которое является специализированным только для целей аутентификации, но поддерживает две разные процедуры аутентификации для двух разных типов транзакции. Устройство 16' имеет две SIM-карты 60, 60′ (или другие запоминающие устройства), которые хранят разные множества данных доступа. Таким образом, каждая из SIM-карт имеет свой собственный номер мобильного телефона, которые могут даже принадлежать двум разным сетям мобильной связи. Каждый номер мобильного телефона присваивается своему типу транзакции. Эти два номера мобильных телефонов могут быть зарегистрированы в двух разных устройствах аутентификации или могут быть зарегистрированы в одном и том же устройстве аутентификации вместе с информацией, определяющей тип транзакции, для которой они должны использоваться.

Кроме того, устройство 16′ имеет две кнопки 48 и 48′ для активирования по выбору одной из двух SIM-карт 60, 60′. Таким образом, пользователь может определить тип транзакции, которую он хочет выполнить, посредством нажатия либо кнопки 48, либо кнопки 48′, чтобы активировать соответствующую SIM-карту и, неявным образом, соответствующую функцию аутентификации. Затем контроллер 44 автоматически

деактивирует функцию аутентификации (SIM-карту) по истечении некоторого временного интервала.

В качестве альтернативы, устройство 16′ может иметь множество SIM-карт (или других идентификационных номеров сетей мобильной связи, таких как IMSI, номер телефона и т.п.), но только один переключатель 48 для активирования функции аутентификации. Тогда некоторый алгоритм, который сохранен в контроллере 44, используется для определения, какая из SIM-карт должна использоваться, например, в зависимости от даты, времени дня и т.п. Идентичный алгоритм используется в устройстве 18 аутентификации, и успешная аутентификация возможна только тогда, когда и мобильное устройство, и устройство аутентификации используют одни и те же контактные данные, соответствующие определенной SIM-карте. Фиг. 10 иллюстрирует полезную модификацию, которая может быть применена к любой из рассмотренных выше схем связи. Обычно запрос на аутентификацию, отправленный от терминала 10 партнеру 12 по транзакции, будет включать в себя не только идентификатор пользователя, но также и пароль, показывающий, что пользователь действительно наделен полномочиями для запрашиваемой услуги. Однако в варианте осуществления, показанном на Фиг. 10, этот пароль передается не через первый канал 14 связи, а через второй или третий канал связи. Это уменьшает риск перехвата комбинации пароля и идентификатора пользователя посредством прослушивания одного из каналов связи.

Например, пароль может быть сконфигурирован один раз в устройстве 18 аутентификации (например, доверенной третьей стороной), и пользователь не должен ни запоминать пароль, ни вводить его для каждой новой транзакции. Когда устройство 18 аутентификации выдает аутентификацию, оно автоматически добавляет пароль, который является подходящим для конкретного партнера 12 по транзакции и, соответственно, запрашиваемой услуги, и пароль будет передан партнеру 12 по транзакции вместе с аутентификацией.

В другом варианте осуществления пароль может постоянно храниться в мобильном устройстве 16 и отправляться устройству 18 аутентификации через канал 20 беспроводной связи на описанном выше этапе D. В варианте осуществления, показанном на Фиг. 10, мобильное устройство вместо этого включает в себя генератор 62 пароля, который формирует динамически изменяющийся пароль в соответствии с некоторым алгоритмом, который зеркально отражается устройством 18 аутентификации. Таким образом, даже если идентификатор IMSI был перехвачен ловушкой IMSI, мошенничество может быть обнаружено вследствие несоответствия паролей, сформированных в мобильном устройстве 16 и устройстве 18 аутентификации, соответственно. Предпочтительно пароль, отправляемый через канал 20 связи, зашифрован.

Кроме того, в показанном примере пароль, сформированный в мобильном устройстве, является универсальным паролем, который используется для каждого процесса аутентификации, независимо от партнера по транзакции и типа используемой услуги. Тогда на основе информации об определенном типе услуги, переданной от партнера 12 по транзакции на этапе B, если аутентификация успешна, устройство 18 аутентификации автоматически преобразует универсальный пароль в заданный пароль, который является подходящим для типа услуги.

В еще одном варианте осуществления, как показано на Фиг. 10, мобильное устройство 16 также включает в себя интерфейс для некоторого идентификационного признака пользователя. В показанном примере интерфейс представляет собой устройство считывания карт для считывания смарт-карты, например, смарт-карты с удостоверением личности или смарт-карты с паспортом пользователя. Пользователь вставляет свою

смарт-карту в устройство считывания карт (или смарт-карта постоянно размещена в устройстве считывания карт), с тем чтобы идентифицирующие данные со смарт-карты могли быть считаны и могли быть переданы через канал 20 связи вместе с паролем или вместо пароля.

Формула изобретения

1. Способ аутентификации пользователя для транзакции в терминале (10), в котором идентификатор пользователя передается от терминала (10) партнеру (12) по транзакции через первый канал (14) связи, и используется второй канал (20) связи для проверки функции аутентификации, которая реализована в мобильном устройстве (16) пользователя, функция аутентификации обычно является не активной и активируется пользователем только предварительно по отношению к транзакции, и в качестве критерия для решения, следует ли выдать или отклонить аутентификацию для транзакции, устройство (18) аутентификации проверяет, существует ли заданное временное отношение между передачей идентификатора пользователя и активным состоянием функции аутентификации, причем способ отличается тем, что устройство (18) аутентификации связывается со вторым каналом (20) связи для проверки активного состояния функции аутентификации и принимает ответ от второго канала связи, причем упомянутый ответ включает в себя информацию о том, что функция аутентификации является активной, и функция аутентификации автоматически деактивируется.

2. Способ по п. 1, в котором функция аутентификации деактивируется после заданного временного интервала после ее активации, и/или когда ее активное состояние было проверено.

3. Способ по п. 1, в котором упомянутая функция аутентификации состоит в регистрации мобильного устройства в сети мобильной связи, которая обеспечивает второй канал связи.

4. Способ по п. 3, в котором сеть мобильной связи разрешает устройству (18) аутентификации обнаруживать зарегистрированное состояние мобильного устройства (16) и, следовательно, активное состояние функции аутентификации посредством проверки только реестра связи сети без необходимости взаимодействия с мобильным устройством (16).

5. Способ по п. 1, в котором устройство (18) аутентификации определяет текущее местоположение мобильного устройства (16) и отклоняет аутентификацию пользователя, когда местоположения терминала (10) и мобильного устройства (16) не соответствуют заданному пространственному отношению.

6. Способ по п. 5, в котором второй канал (20) связи включает в себя сеть мобильной связи, поддерживающую услуги на основе местоположения, и устройство (18) аутентификации использует эти услуги на основе местоположения для определения местоположения мобильного устройства (16).

7. Способ по п. 5, в котором мобильное устройство (16) обнаруживает свое собственное местоположение и отправляет информацию о местоположении устройству (18) аутентификации.

8. Способ по п. 1, в котором устройство (18) аутентификации определяет текущее местоположение мобильного устройства (16) и аутентифицирует пользователя, когда местоположения терминала (10) и мобильного устройства (16) соответствуют заданному пространственному отношению, и активное состояние функции аутентификации в мобильном устройстве проверяется только тогда, когда упомянутое пространственное отношение не выполняется.

9. Способ по п. 1, в котором устройство (18) аутентификации является удаленным от партнера (12) по транзакции и взаимодействует с партнером по транзакции через третий канал (22) связи, и в котором информация, привязывающая идентификатор пользователя к адресу мобильного устройства (16) в сети мобильной связи, хранится только в устройстве (18) аутентификации, и устройство аутентификации уведомляет партнера (12) по транзакции только о том, аутентифицирован ли пользователь, не раскрывая дополнительные данные, принадлежащие пользователю и/или мобильному устройству (16).

10. Способ по п. 1, в котором пароль передается партнеру (12) по транзакции через устройство (18) аутентификации.

11. Способ по п. 10, в котором пароль хранится или формируется в мобильном устройстве (16) и передается устройству (18) аутентификации.

12. Способ по п. 10, в котором пароль хранится или преобразуется в устройстве (18) аутентификации.

13. Способ по п. 1, в котором мобильное устройство (16) соединено интерфейсом с идентифицирующим признаком пользователя для считывания из него идентифицирующих данных, и эти идентифицирующие данные передаются устройству (18) аутентификации через второй канал (20) связи.

14. Мобильное устройство (16) для использования в способе аутентификации по любому из пп. 1-9, содержащее беспроводной приемопередатчик (40), переключатель (48) и электронный контроллер (44), который реализует упомянутую функцию аутентификации и выполнен с возможностью активирования функции аутентификации в ответ на управление переключателем (48) и деактивирования ее после того, как она была активна в течение заданного временного интервала, или после проверки ее состояния.

15. Устройство по п. 14, дополнительно содержащее аккумулятор (46) и разъем (52) для соединения аккумулятора (46) с источником напряжения.

16. Устройство по п. 15, содержащее дисплей (47) для индикации состояния заряда аккумулятора (46).

17. Устройство по п. 15, в котором разъем (52) является разъемом USB или разъемом микро-USB.

18. Устройство по п. 15, в котором разъем (52) является штепсельным разъемом, закрытым съемной крышкой (54), которая включает в себя два гнездовых разъема (56, 58), позволяющих соединить штепсельный разъем (52) с источником напряжения через один (56)из гнездовых разъемов, в то время как другой (58) из гнездовых разъемов соединен со штепсельным разъемом (52).

19. Устройство по п. 14, содержащее функцию позиционирования для беспроводного обнаружения своей собственной позиции, причем функция аутентификации включает в себя функцию отправки обнаруженного местоположения через приемопередатчик (40).

20. Устройство по п. 14, в котором функция аутентификации состоит только из активирования и деактивирования приемопередатчика (40).

21. Устройство по п. 14, содержащее корпус (38), который заключает в себе по меньшей мере контроллер (44) и предотвращает доступ к нему.

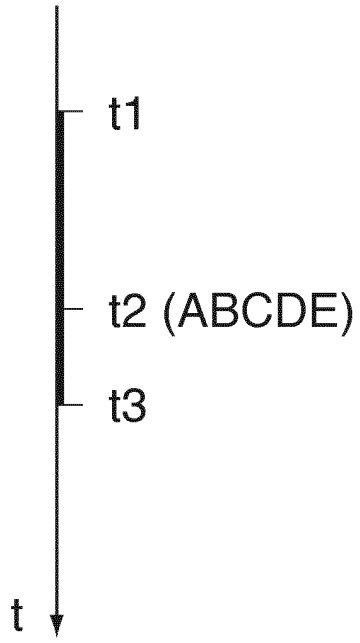
22. Устройство по п. 14, содержащее функцию самоуничтожения, выполненную с возможностью активирования посредством попытки принудительного доступа.

23. Устройство по п. 14, в котором приемопередатчик (40) представляет собой единственный порт ввода и вывода данных контроллера (44).

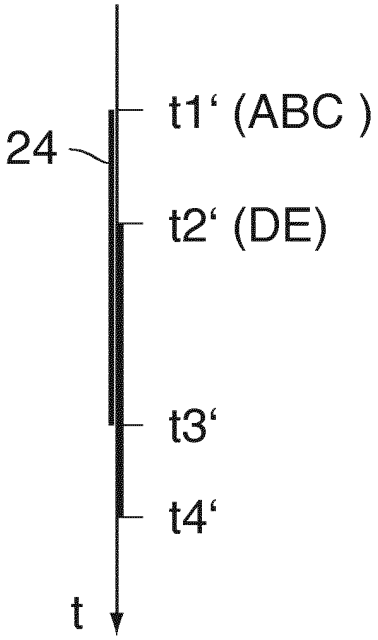
24. Устройство по п. 14, содержащее средство (60, 60′) хранения для множества адресов мобильной связи и средство (48, 48′) ввода, включающее в себя переключатель (48) и выполненное с возможностью активирования по выбору одной из множества функций аутентификации, каждая из которых присвоена своему одному из упомянутых адресов мобильной связи.

25. Устройство по п. 14, содержащее средство (60, 60′) хранения для множества адресов мобильной связи, причем контроллер (44) выполнен с возможностью выбора одного из множества адресов мобильной связи в соответствии с заданным алгоритмом.

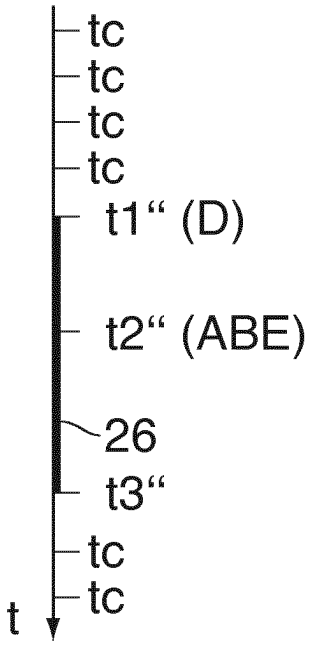
26. Устройство по п. 14, содержащее акустический преобразователь (49) для обеспечения акустического сигнала обратной связи при активировании и/или деактивировании функции аутентификации.



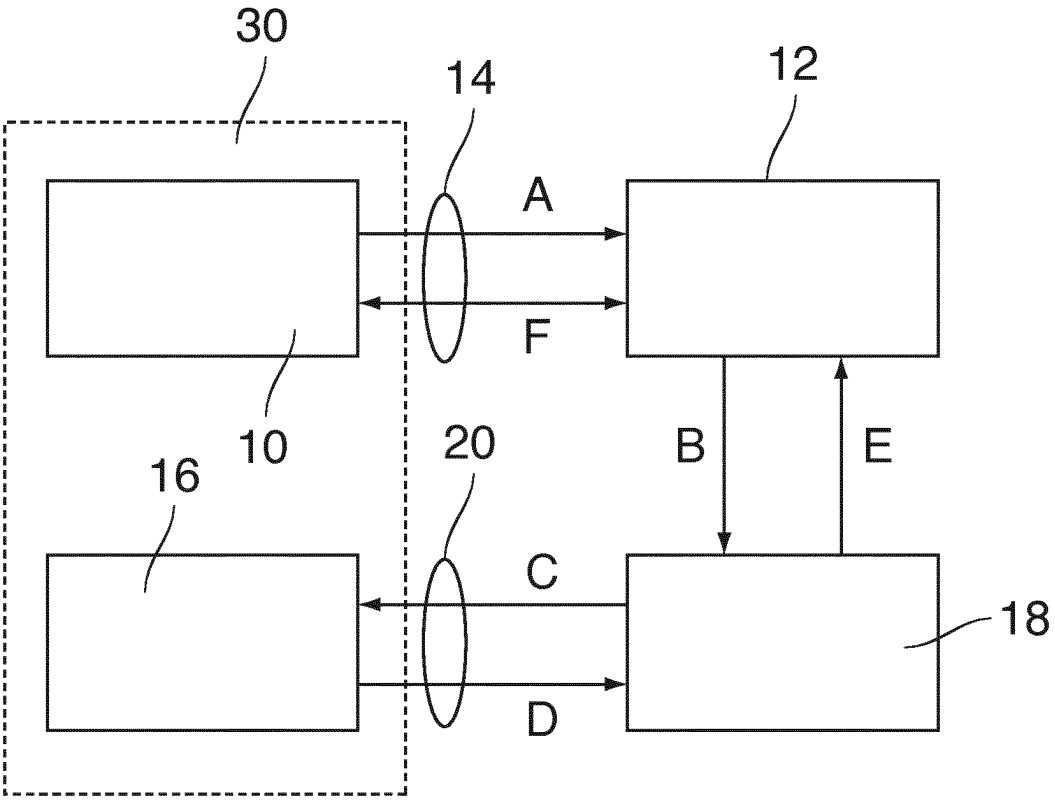
Фиг. 2



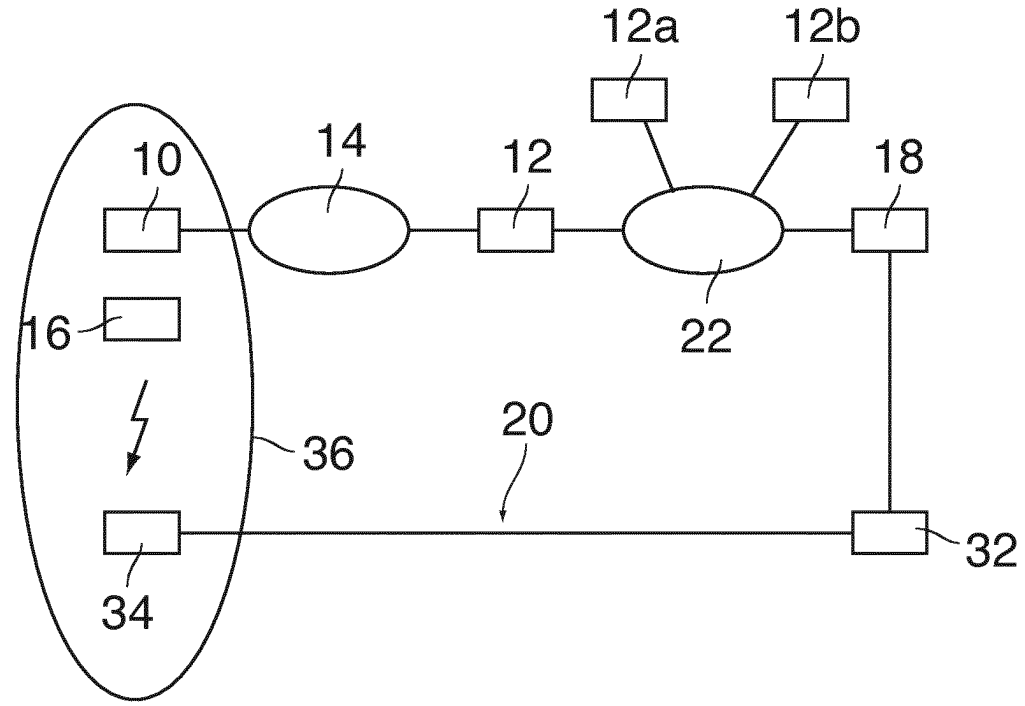
Фиг. 3



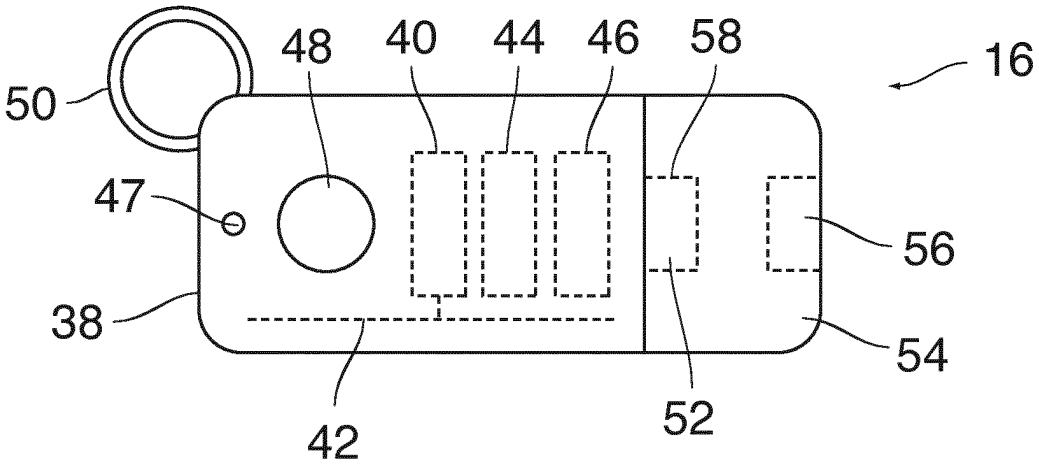
Фиг. 4



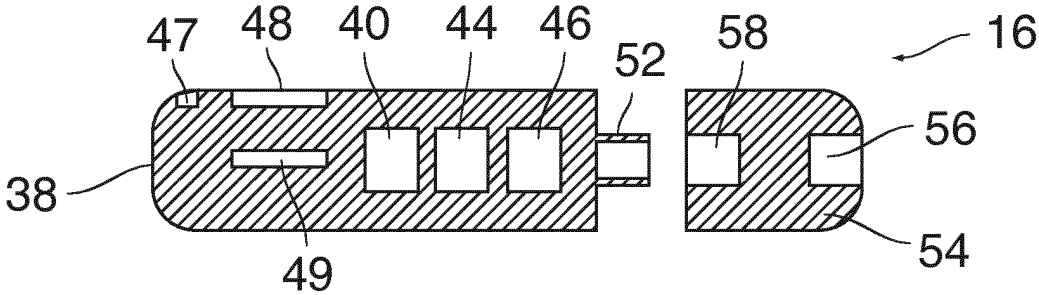
Фиг. 5



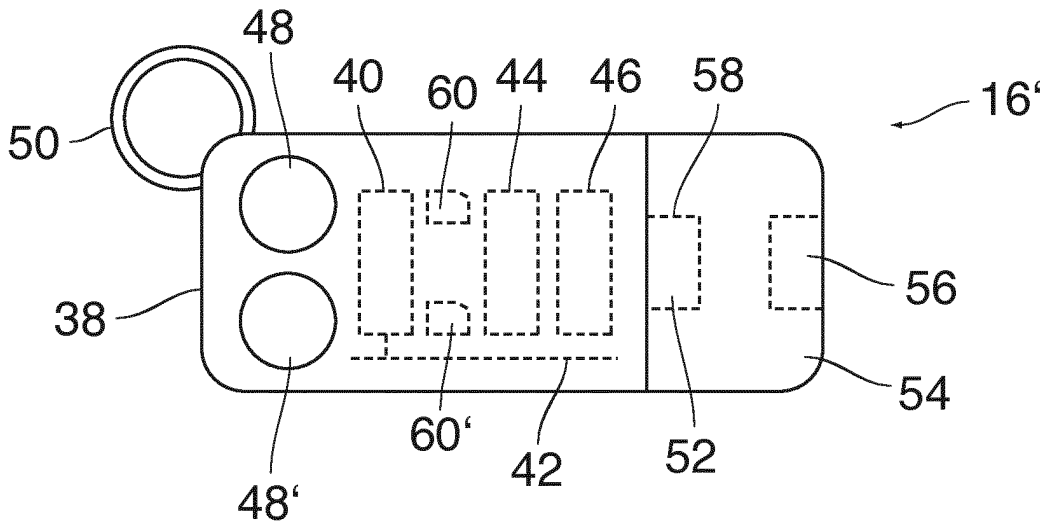
Фиг. 6



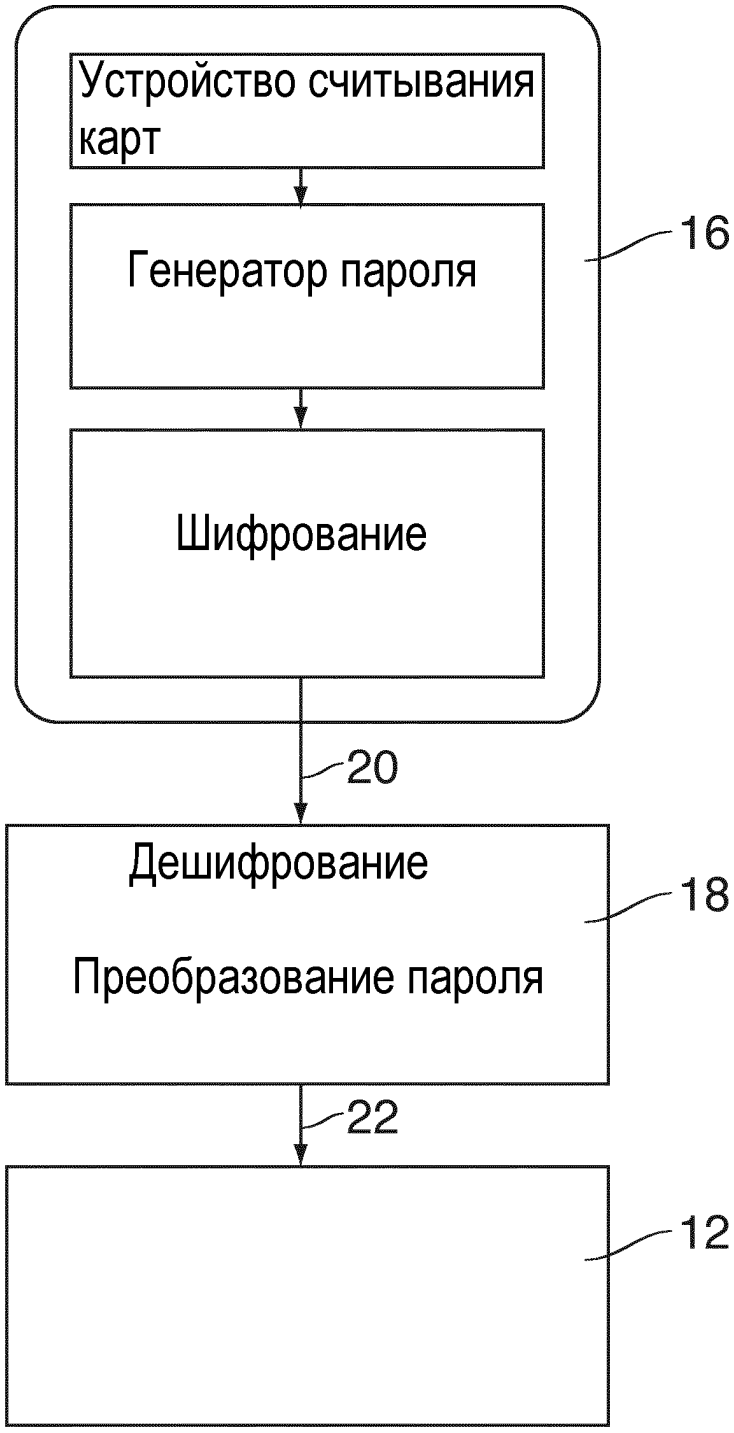
Фиг. 7



Фиг. 8



Фиг. 9


Устройство считывания карт
Генератор пароля
Шифрование
16
20
Дешифрование
Преобразование пароля
18
22
12

Фиг. 10