(19) Евразийское патентное ведомство

(11) 036987 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2021.01.25

(21) Номер заявки
201990708

(22) Дата подачи заявки
2017.09.08

(51) Int. Cl. ***H04L 9/32*** (2006.01)
H04L 9/14 (2006.01)
H04L 9/30 (2006.01)
H04L 29/06 (2006.01)
H04W 12/04 (2009.01)

(54) СИСТЕМЫ И СПОСОБЫ ДЛЯ АУТЕНТИФИКАЦИИ УСТРОЙСТВ

(31) **62/393,438; 62/423,593; 15/395,336; 15/634,265**
(32) **2016.09.12; 2016.11.17; 2016.12.30; 2017.06.27**
(33) **US**
(43) **2019.10.31**
(86) **PCT/US2017/050614**
(87) **WO 2018/049116 2018.03.15**

(71)(73) Заявитель и патентовладелец:
ИНФОСКИ, ЛЛС (US)

(72) Изобретатель:
Эллингсон Джон, Оттосон Томас Чарльз (US)

(74) Представитель:
Рыбина Н.А., Рыбин В.Н. (RU)

(56) US-B1-8855312
US-B2-8510565
US-A1-20160156614
US-B2-9432198
US-A1-20140057601

(57) Воплощения включают способы, системы и устройства для обработки данных, сконфигурированные для реализации способов аутентификации устройства для обработки данных. Процессор первого устройства для обработки данных может получать временный идентификатор и может отправлять временный идентификатор на второе устройство для обработки данных и третье устройство для обработки данных. Процессор второго устройства для обработки данных может отправлять временный идентификатор на третье устройство для обработки данных с запросом на аутентификацию первого устройства для обработки данных. Процессор третьего устройства для обработки данных может аутентифицировать идентификатор первого устройства для обработки данных в ответ на определение того, что временный идентификатор, принятый от первого устройства для обработки данных, соответствует временному идентификатору, принятому от второго устройства для обработки данных.

036987 B1

036987 B1

Уровень техники

Концепция общих секретов и сопутствующего доверия была краеугольным камнем парадигмы безопасности еще до падения Трои. Исторически общий секрет представлял собой пароль, который две стороны могли использовать, чтобы отличить друг друга, в качестве меры доверия. Хотя эти общие секреты могли меняться время от времени, они были достаточно долговечными, чтобы существовать от момента обмена ими до момента использования. Пароли работали только при условии, что они хранятся в секрете. Стороны, которые обменивались секретами, обычно были некоторым образом известны друг другу или, в ином случае, за них ручались. Использование пароля и отзыва позволяло идентифицировать доверенные стороны в темноте или за счет использования надежного общего секрета. Доверие могло быть оказано другому лицу в результате разрешенной передачи секрета.

В последнее время развитие цифровой среды позволило, помимо прочего, добиться значительного расширения быстрой связи и информационных транзакций. Старая парадигма общего секрета была включена в цифровую среду множеством способов - от имен пользователя и паролей до защищенной связи между пользователями и системами. Например, эта концепция является фундаментальной для уровня защищенных сокетов и инфраструктуры защиты информации сертифицирующих органов.

Однако цифровая среда - это среда, в которой секреты трудно хранить дольше короткого периода времени, и после потери секретности ранее секретная информация может быстро распространяться с полной достоверностью. Также в цифровой среде общие секреты становятся объектом "взлома", в результате которого многие "секреты" (например, пароли, цифровые сертификаты, личная информация и другие типы аутентификационных данных) превращаются в товар, который свободно продается на "сером" и "черном" рынках, что сводит на нет преимущество таких секретов для обеспечения безопасности цифрового обмена данными. Тем не менее, лежащий в основе механизм обеспечения безопасности цифровой среды зависит от рабочего, но часто ошибочного предположения о том, что секрет все еще остается тайным. Новая динамика несостоятельности парадигмы общего секрета и зависящего от нее доверия требует радикального изменения рабочих предположений.

Сущность изобретения

Различные воплощения включают способы аутентификации взаимодействий между первым устройством для обработки данных и вторым устройством для обработки данных с помощью третьего устройства для обработки данных. Различные воплощения могут включать получение первого временного идентификатора на первом устройстве для обработки данных, отправку первого временного идентификатора на второе устройство для обработки данных и на третье устройство для обработки данных, прием на втором устройстве для обработки данных первого временного идентификатора от первого устройства для обработки данных, получение второго временного идентификатора на втором устройстве для обработки данных, отправку второго временного идентификатора от второго устройства для обработки данных на первое устройство для обработки данных и на третье устройство для обработки данных, прием на первом устройстве для обработки данных второго временного идентификатора от второго устройства для обработки данных, отправку запроса на аутентификацию, включающего второй временный идентификатор, от первого устройства для обработки данных на третье устройство для обработки данных, отправку запроса на аутентификацию, включающего первый временный идентификатор, от второго устройства для обработки данных на третье устройство для обработки данных, прием на третьем устройстве для обработки данных первого временного идентификатора от первого устройства для обработки данных, прием на третьем устройстве для обработки данных от второго устройства для обработки данных запроса на аутентификацию, содержащего первый временный идентификатор, определение на третьем устройстве для обработки данных того, соответствует ли первый временный идентификатор от второго устройства для обработки данных первому временному идентификатору от первого устройства для обработки данных, отправку третьим устройством для обработки данных на второе устройство для обработки данных указания того, аутентифицировано ли первое устройство для обработки данных, на основании определения того, соответствует ли первый временный идентификатор от второго устройства для обработки данных первому временному идентификатору от первого устройства для обработки данных, прием на третьем устройстве для обработки данных второго временного идентификатора от второго устройства для обработки данных, прием на третьем устройстве для обработки данных запроса на аутентификацию, содержащего второй временный идентификатор, от первого устройства для обработки данных, определение третьим устройством для обработки данных того, соответствует ли второй временный идентификатор от первого устройства для обработки данных второму временному идентификатору от второго устройства для обработки данных, отправку третьим устройство для обработки данных на первое устройство для обработки данных указания того, аутентифицировано ли второе устройство для обработки данных, на основании определения того, соответствует ли второй временный идентификатор от первого устройства для обработки данных второму временному идентификатору от второго устройства для обработки данных, прием на первом устройстве для обработки данных от третьего устройства для обработки данных указания того, аутентифицировано ли второе устройство для обработки данных, и прием на втором устройстве для обработки данных от третьего устройства для обработки данных указания того, аутентифицировано ли первое устройство для обработки данных.

Различные воплощения дополнительно включают устройства для обработки данных, сконфигурированные с выполняемыми процессором инструкциями для выполнения операций способа, описанных выше. Различные воплощения дополнительно включают систему, содержащую первое устройство для обработки данных, второе устройство для обработки данных и третье устройство для обработки данных, все из которых сконфигурированы для выполнения операций способа, описанных выше.

Краткое описание чертежей

Прилагаемые чертежи, включенные в настоящий документ и составляющие часть настоящего описания, показывают примерные воплощения изобретения и вместе с общим описанием, приведенным выше, и подробным описанием, приведенным ниже, служат для объяснения особенностей изобретения.

Фиг. 1A-1C - блок-схемы компонентов системы связи, подходящей для применения в различных воплощениях.

Фиг. 2 - блок-схема компонентов устройства связи, подходящего для применения в различных воплощениях.

Фиг. 3A - технологическая блок-схема, показывающая способ аутентификации одного устройства для обработки данных относительно другого устройства для обработки данных согласно различным воплощениям.

Фиг. 3B - схема передачи сообщений, показывающая другой способ аутентификации одного устройства для обработки данных относительно другого устройства для обработки данных согласно различным воплощениям.

Фиг. 3C - блок-схема способа 300a операций, выполняемых первым устройством для обработки данных как часть способа 300.

Фиг. 3D - блок-схема способа 300b операций, выполняемых вторым устройством для обработки данных как часть способа 300.

Фиг. 3E - блок-схема способа 300c операций, выполняемых третьим устройством для обработки данных как часть способа 300.

Фиг. 4A - технологическая блок-схема, показывающая способ аутентификации одного устройства для обработки данных относительно другого устройства для обработки данных и авторизации информационной транзакции между двумя устройствами согласно различным воплощениям.

Фиг. 4B - блок-схема способа 400a операций, выполняемых первым устройством для обработки данных как часть способа 400.

Фиг. 4C - блок-схема способа 400b операций, выполняемых вторым устройством для обработки данных как часть способа 400.

Фиг. 4D - блок-схема способа 400c операций, выполняемых третьим устройством для обработки данных как часть способа 400.

Фиг. 5A - технологическая блок-схема, показывающая способ защиты связи между двумя устройствами для обработки данных в случае вторжения неавторизованной стороны согласно различным воплощениям.

Фиг. 5B - блок-схема способа 500a операций, выполняемых третьим устройством для обработки данных как часть способа 500.

Фиг. 6A - технологическая блок-схема, показывающая способ аутентификации одного устройства для обработки данных относительно другого устройства для обработки данных согласно различным воплощениям.

Фиг. 6B - блок-схема способа 600a операций, выполняемых первым устройством для обработки данных как часть способа 600.

Фиг. 6C - блок-схема способа 600b операций, выполняемых вторым устройством для обработки данных как часть способа 600.

Фиг. 6D - блок-схема способа 600c операций, выполняемых третьим устройством для обработки данных как часть способа 600.

Фиг. 7 - блок-схема компонентов мобильного беспроводного устройства для обработки данных, подходящего для реализации различных воплощений.

Фиг. 8 - блок-схема компонентов портативного устройства беспроводной связи, подходящего для реализации различных воплощений.

Фиг. 9 - блок-схема компонентов серверного устройства, подходящего для реализации различных воплощений.

Подробное описание

Различные воплощения будут подробно описаны со ссылкой на прилагаемые чертежи. По возможности, для обозначения одинаковых или подобных деталей на всех чертежах будут использоваться одинаковые ссылочные номера. Ссылки на конкретные примеры и воплощения приведены лишь для иллюстративных целей и не должны рассматриваться как ограничивающие объем изобретения или формулы.

В различных воплощениях предлагаются способы и устройства для обработки данных (или другие цифровые или программируемые устройства), сконфигурированные для реализации способов, которые обеспечивают аутентификацию устройства для обработки данных относительно других устройств для

обработки данных в системе связи на основании динамической информации устройства для обработки данных, которая не основана на парадигме общих секретов и статической информации. Поскольку временный идентификатор каждого устройства для обработки данных периодически или апериодически меняется, и каждое устройство для обработки данных периодически или апериодически находится на связи с другими устройствами для обработки данных, (синхронно или асинхронно) отправляющими и/или принимающими новые временные идентификаторы, различные воплощения улучшают работу любой сети связи или любой системы электронной связи за счет повышения уровня безопасности связи. Различные воплощения также улучшают работу любой сети связи за счет надежной аутентификации идентификатора задействованного устройства для обработки данных, не опираясь на статическую идентификационную информацию, такую как общий секрет, которая может быть уязвимой к атаке в результате доступа и/или копирования.

Термин "устройство для обработки данных" относится к любому программируемому компьютеру или процессору, который может быть сконфигурирован с программируемыми инструкциями для выполнения способов согласно различным воплощениям. Устройство для обработки данных может включать в себя одно или все из персональных компьютеров, портативных компьютеров, планшетных компьютеров, сотовых телефонов, смартфонов, сотовых телефонов с выходом в Интернет, электронных устройств с доступом к Wi-Fi, карманных персональных компьютеров (PDA), носимых устройств для обработки данных (включая умные часы, ожерелья, медальоны и любое устройство для обработки данных, предназначенное для ношения, прикрепляемое к носимому предмету или встраиваемое в носимый предмет), беспроводных вспомогательных устройств, беспроводных периферийных устройств, устройств "Интернета вещей" (IoT), сетевых элементов, таких как серверы, маршрутизаторы, шлюзы и т.п. (включая так называемые "облачные" устройства для обработки данных), и аналогичных электронных устройств, оснащенных радиоприбором ближнего действия (например, радиоприбор Bluetooth, Peanut, ZigBee и/или Wi-Fi и т.п.) и/или подключением к глобальной вычислительной сети (например, с помощью одной или более технологий сотового радиодоступа для связи с помощью беспроводного приемопередатчика глобальной вычислительной сети или проводного подключения к сети связи).

В контексте настоящего документа термин "информационная транзакция" относится к любой связи или обмену информацией, в котором идентификатор задействованных устройств может быть аутентифицирован. В некоторых воплощениях способы и устройства для обработки данных, сконфигурированные для реализации способов, описанных в настоящем документе, могут быть реализованы во множестве случаев, в которых идентификатор задействованных устройств может быть аутентифицирован, например, в ведении медицинских архивов, защищенной связи (например, в сфере правительства, бизнеса, разведки и т.д.), системах ведения общественных архивов, системах голосования, системах финансового обслуживания, системах обеспечения безопасности брокерской деятельности и многих других. В некоторых воплощениях способы и устройства для обработки данных, сконфигурированные для реализации способов, описанных в настоящем документе, могут быть реализованы в устройствах IoT или между устройствами IoT и контроллером устройств IoT, такими как маршрутизатор, сервер, концентратор IoT или другое аналогичное устройство. В частности, различные воплощения при реализации в среде IoT могут быть особенно полезны при предотвращении распределенных атак типа "отказ в обслуживании" (DDoS) без человеческого вмешательства. В некоторых воплощениях способы и устройства для обработки данных, сконфигурированные для реализации способов, описанных в настоящем документе, могут аутентифицировать участие устройства для обработки данных в информационной транзакции. В некоторых воплощениях способы и устройства для обработки данных, сконфигурированные для реализации способов, описанных в настоящем документе, могут быть реализованы в контексте коммерческой операции для осуществления неопровержимой коммерческой операции, в которой, поскольку участие определенных устройств для обработки данных может быть аутентифицировано, участник не сможет впоследствии отрицать свое участие в операции (такой как, например, финансовая операция, совершаемая без участия карты).

Термины "компонент", "система" и т.п. включают относящийся к компьютеру объект, такой как, без ограничения, аппаратное обеспечение, программно-аппаратное обеспечение, комбинация аппаратного обеспечения и программного обеспечения, программное обеспечение или выполняемое программное обеспечение, которые сконфигурированы для выполнения конкретных операций или функций. Например, компонент может представлять собой, без ограничения, процесс, запущенный на процессоре, процессор, объект, исполнимый модуль, поток исполнения, программу и/или компьютер. В качестве иллюстрации компонентом может считаться как приложение, запущенное на беспроводном устройстве, так и само беспроводное устройство. Один или более компонентов могут находиться в процессе и/или поток исполнения и компонент могут быть локально расположены на одном процессоре или ядре и/или распределены между двумя или более процессорами или ядрами. Кроме того, эти компоненты могут исполняться из различных постоянных машиночитаемых носителей, на которых хранятся различные инструкции и/или структуры данных. Компоненты могут связываться посредством локальных и/или удаленных процессов, функции или вызовов процедуры, электронных сигналов, пакетов данных, считываний из памяти/записей в память и других известных методик связи, связанных с компьютером, процессором

и/или процессом.

Цифровая среда обеспечивает возможность осуществления, помимо прочего, быстрой связи и информационных транзакций вплоть до глобального масштаба. Однако имеющаяся в настоящее время цифровая среда опирается на шаткую основу обеспечения безопасности: старую парадигму статического общего секрета. Существует множество фундаментальных отличий между чисто человеческой средой, в которой совершались операции тысячи лет, и цифровой средой, в которой осуществляются операции в настоящее время.

Пятьдесят лет назад коммерция и обмен данными часто совершались лицом к лицу, на локальном уровне и между сторонами, знающими друг друга. В настоящее время коммерция и обмен данными осуществляются на расстоянии, на глобальном масштабе и между сторонами, которые не только не знают друг друга, но возможно и никогда не встретятся, т.е. цифровая среда, как правило, является анонимной и удаленной, а не локальной и знакомой. Кроме того, многие современные операции цифровой связи осуществляются между устройствами для обработки данных, действующими независимо от взаимодействий с человеком или человеческих знаний. Операции в присутствии обеих сторон обычно включают этап аутентификации, визуального распознания другой стороны. При осуществлении операций между полными незнакомцами, совершенно неизвестными друг другу и находящимися на расстоянии друг от друга, переход от аналоговой среды, включающей взаимодействия среди известных сторон, к цифровой среде предусматривал уязвимость, которая является характерной, хотя и часто непризнанной, и заключается в том, что аутентификация сторон включает способы, осуществляемые при помощи компьютера, которые могут быть скомпрометированы.

Кроме того, цифровая среда - это среда, в которой секреты трудно хранить дольше короткого периода времени. После потери секретности ранее секретная информация может быстро распространяться с полной достоверностью. Бреши в безопасности цифровых систем, приводящие к массивным утечкам данных, стали практически обычным явлением, и частота их возникновения возросла.

В большинстве случаев со сбоями причиной нарушения безопасности является несоблюдение принципов доверия или неправильное использование общего секрета (например, учетных данных). Хотя в некоторых случаях конкретное нарушение безопасности может быть связано с нехваткой стойкости технологии, используемой для обеспечения доверия и безопасности, в целом нарушения безопасности в цифровой среде происходили в самых различных отраслях с использованием множества внедряемых технологий. Нарушения безопасности происходят по всем аспектам и связаны не только с какой-либо конкретной внедряемой технологией, но также с практическими реализациями и процедурами, присущими ее применению и использованию. Таким образом, нарушения безопасности в цифровой среде происходят из-за чего-то более фундаментального и характерного в корневой стратегии парадигмы доверия общего секрета, которая дала сбой.

Текущая парадигма цифровой безопасности не работает по меньшей мере по трем основным причинам: (1) текущая парадигма основана на доверии, но доверие не дает нужного результата; (2) текущая парадигма основана на постоянных или статичных общих секретах, но секреты не остаются в тайне; и (3) подавляющее большинство информационных транзакций осуществляется между анонимными сторонами. Таким образом, "основанные на доверии системы" совершенно не работают, поскольку они могут быть взломаны и являются уязвимыми. Более того, текущие "основанные на доверии системы" являются уязвимыми к вторжению и расшифровке большей частью из-за использования статичной или длительно используемой информации, которая не меняется с течением времени (или промежутка времени).

Например, текущая парадигма цифровой безопасности основана на сертифицирующем органе или аналогичном органе, который выдает статический цифровой сертификат (или любые другие аналогичные данные). Цифровой сертификат может удостоверять владение открытым ключом по названному субъекту сертификата, формально позволяя другим сторонам полагаться на подписи или утверждения, сделанные в отношении закрытого ключа, который соответствует сертифицированному открытому ключу. Один пример этой парадигмы безопасности представляет собой уровни защищенных сокетов (SSL), протокол обеспечения безопасности, широко используемый для обеспечения безопасности связи между устройствами для обработки данных, например, между веб-браузером на устройстве для обработки данных и удаленным веб-сервером. SSL применяет криптографическую систему, которая использует открытый ключ и закрытый ключ для шифрования информации, передаваемой между устройством для обработки данных и сайтом. Принцип обеспечения безопасности SSL основан на сертификатах, выдаваемых сертифицирующим органом, которые устанавливаются на сервере компании после аттестации компании сертифицирующим органом. В этой модели доверительных отношений сертифицирующий орган представляет собой третью сторону, которой доверяет как владелец сертификата, так и другая сторона, полагающаяся на сертификат.

К основным слабым местам в этой парадигме безопасности относятся сертификат и сертифицирующий орган. Если сертификат на устройстве для обработки данных скомпрометирован, то безопасность передачи данных от этого устройства для обработки данных или на него утрачивается. Если скомпрометирован сертифицирующий орган, то утрачивается безопасность всей системы, что потенциально ставит под угрозу все субъекты, которые доверяют скомпрометированному сертифицирующему органу.

Злоумышленник, который получает доступ к сертификатам от скомпрометированного сертифицирующего органа, может затем выдать себя за любого доверенного пользователя, представленного сертифицирующим органом. Таким образом, использование статических сертификатов создает возможность для катастрофического нарушения безопасности.

В качестве другого примера множество отдельных устройств может пытаться войти в службу или систему с использованием тех же учетных данных независимо от того, как получены эти учетные данные, но только одно устройство или система могут законно аутентифицировать вход - законный владелец учетных данных. Были разработаны многочисленные стратегии, позволяющие воспользоваться этим принципом, но все они являются неудовлетворительными, поскольку имеют общую уязвимость - этап аутентификации основан на информации, которую злоумышленник может украсть и использовать. Как правило, учетные данные для входа в систему состоят из имени пользователя и пароля. Хотя существует множество средств защиты учетных данных для входа в систему, которые усложняют учетные данные, такие как одноразовое использование и многофакторное использование, все эти используемые способы запутывания или усложнения учетных данных для входа в систему в конечном итоге уязвимы, если сама цифровая инфраструктура уязвима. Само существование и использование этапов многофакторной аутентификации и путей многофакторной аутентификации являются признанием того, что комбинации имени пользователя и пароля не соответствуют задаче обеспечения безопасности.

Различные воплощения, раскрытые в этой заявке, решают проблему уязвимости безопасности цифровых систем и обеспечивают электронную безопасность для связи между устройствами, а также для улучшенной аутентификации пользователя. Различные воплощения предоставляют реализуемые на компьютере способы для обеспечения постоянного обновления и изменения цифровых сертификатов. Различные воплощения включают предположение, что основанные на доверии системы в конечном счете явно небезопасны, поскольку такие системы могут быть взломаны и являются уязвимыми. Различные воплощения обеспечивают цифровую систему связи, которая не предполагает доверия между различными сетевыми элементами, по меньшей мере по той причине, что цифровая среда по своей природе ненадежна.

В различных воплощениях изменяют способ аутентификации устройств в сетях путем генерирования и совместного использования аутентифицирующей информации такого ограниченного срока действия, что она не может быть эффективно использована злоумышленником. В различных воплощениях срок действия, в течение которого аутентифицирующая информация может использоваться, может быть относительно коротким, например срок действия может исчисляться в минутах. Это идет вразрез с эффективным сроком действия сертификатов от обычного сертифицирующего органа (CA), который в некоторых случаях может иметь продолжительность до нескольких десятков лет. В некоторых воплощениях срок действия аутентифицирующей информации может быть определен как более короткий, чем время, которое требуется злоумышленнику для получения и использования информации. Различные воплощения основаны на предположении, что аутентифицирующая информация потенциально уязвима и может быть получена злоумышленником, и срок действия аутентифицирующей информации может быть определен так, что ее целесообразность для аутентификации истекает до того, как нарушитель сможет обнаружить и использовать ее. Например, на основе современных вычислительных возможностей может быть определено количество времени, необходимое для расшифровки обычно используемого хеша шифрования (например, SHA256) с использованием перебора. В различных воплощениях срок действия аутентифицирующей информации может изменяться, поскольку усовершенствования в вычислительных технологиях сокращают время, необходимое для обнаружения и расшифровки такой информации. В некоторых воплощениях система может определять срок действия аутентифицирующей информации, который короче определенного времени, необходимого для расшифровки зашифрованной информации.

Относительно короткий используемый срок действия аутентифицирующей информации на несколько порядков уменьшает вероятность того, что такая аутентифицирующая информация будет угадана, доступна или "взломана", а затем использована в качестве средства для атаки на систему. Использование такой аутентифицирующей информации позволяет системе авторизовать только необходимые устройства и запрещать доступ к неавторизованным устройствам, даже когда такие неавторизованные устройства предоставляют ранее приемлемые имя пользователя и пароли, сертификаты или другие учетные данные для доступа. Таким образом, различные воплощения дополнительно позволяют существующим технологиям и компонентам обеспечения безопасности не допускать получения доступа к устройству или системе злоумышленниками, которые получили точные копии подлинных учетных данных пользователя для входа в систему. Различные воплощения могут применяться в других приложениях обеспечения безопасности, использующих одноразовые пароли, таких как обеспечение безопасности облачного сервиса, а также на широком спектре устройств, включая устройства Интернета вещей (IoT). Различные воплощения могут применяться для аутентификации связи между различными устройствами, такими как устройства для обработки данных, которые могут быть объектами атаки или подчинения для участия при выполнении распределенной атаки типа "отказ в обслуживании" (DDoS).

В различных воплощениях устройства для обработки данных выполняют двунаправленную, трехстороннюю аутентификацию, в которой каждое устройство для обработки данных периодически (или

апериодически) генерирует эфемерный "временный идентификатор" с использованием аспектов динамических и/или статических состояний (отдельно или в комбинации) устройства для обработки данных. Временные идентификаторы, генерируемые каждым устройством для обработки данных, могут обмениваться и аутентифицироваться двумя (или более) другими устройствами для обработки данных. Временные идентификаторы могут использоваться с существующими методиками обеспечения безопасности, включая способы хеширования, обновленные ключи, обновленные точки доверия, сопоставление сертификатов клиентов, службу каталогов Active Directory, сопоставление сертификатов клиентов служб Internet Information Services (IIS), цифровые сертификаты, доверенную третью сторону и другие механизмы обеспечения безопасности. Различные воплощения могут не допускать попыток выдавать себя за авторизованное устройство для обработки данных, таких как попытка входа в компьютерную сеть или онлайн-среду со стороны неавторизованного пользователя, обладающего учетными данными авторизованного пользователя. Различные воплощения также могут обеспечивать безопасную связь между цифровыми устройствами любого типа в любой сети. Таким образом, различные воплощения могут обеспечивать безопасную, надежную и аутентифицированную связь между устройствами для обработки данных в сети связи, которая устраняет общие уязвимости традиционных технологий аутентификации.

В различных воплощениях временный идентификатор может быть сгенерирован динамически, например, по меньшей мере, частично на основе одного или более изменяющихся или динамических состояний устройства для обработки данных, которое генерирует временный идентификатор, или динамической информации, полученной датчиком в устройстве для обработки данных (например, камере, микрофоне, акселерометре и т.д.). В некоторых воплощениях устройство для обработки данных может генерировать свой собственный временный идентификатор. В некоторых воплощениях другое устройство для обработки данных, такое как сервер аутентификации, может генерировать временный идентификатор для устройства для обработки данных, и временный идентификатор может быть отправлен на устройство для обработки данных или принят с сервера устройством для обработки данных.

В некоторых воплощениях указанный временный идентификатор может использоваться только один раз. В таких воплощениях временный идентификатор, который был использован, затем может быть непригоден к использованию.

В различных воплощениях время является критическим элементом временных идентификаторов. Например, истечение срока действия временного идентификатора может быть ограничено приемлемым периодом времени, в течение которого можно ожидать сохранение секрета. В различных воплощениях устройство для обработки данных может определять временные рамки или срок действия временного идентификатора, вследствие чего временный идентификатор используется в течение периода времени, который короче времени, необходимого злоумышленнику, чтобы угадать или получить временный идентификатор и использовать его для успешной атаки, например, для получения доступа к защищенной сети или совершения защищенной транзакции. За пределами временных рамок или срока действия временный идентификатор может быть непригодным к использованию для аутентификации любого устройства для обработки данных. Срок действия временного идентификатора может быть короче, чем срок действия указанного сеанса связи (например, сеанса VPN или сеанса покупок через Интернет). В таких ситуациях новый временный идентификатор может быть сгенерирован для устройства для обработки данных во время сеанса связи и использован для обеспечения безопасности обмена данными в сеансе связи после истечения срока действия старого временного идентификатора.

В некоторых воплощениях динамические аспекты генерирующего устройства для обработки данных, используемого для генерирования временных идентификаторов, будут меняться часто или непрерывно таким образом, что каждый временный идентификатор будет основан на разных (т.е. измененных) данных. В таких воплощениях каждый сгенерированный временный идентификатор может содержать уникальные данные (которые могут быть представлены последовательностью данных), которые представляют "снимок" динамического состояния генерирующего устройства для обработки данных в момент генерирования временного идентификатора. В различных воплощениях используются уникальные данные (или уникальная последовательность данных), сгенерированные в соответствии с одним или более постоянно меняющимися условиями в качестве основы для генерирования уникального динамического сертификата. В результате, злоумышленник не сможет обнаружить основу для генерирования временных идентификаторов в попытке сгенерировать поддельные идентификаторы.

В некоторых воплощениях устройства для обработки данных могут обмениваться информацией или иным образом согласовывать время, когда каждое устройство для обработки данных может генерировать новый временный идентификатор. В некоторых воплощениях устройство для обработки данных (например, сервер) может отдавать инструкцию другому устройству для обработки данных (например, пользовательскому устройству) на генерирование нового временного идентификатора. Такая координация генерирования новых временных идентификаторов может обеспечить частые изменения временных идентификаторов во время продолжительного сеанса цифровой связи.

В некоторых воплощениях устройство для обработки данных может содержать модуль, такой как модуль генерирования временного идентификатора, который может хранить небольшой фрагмент статической информации. Информация может включать текст, изображение, биометрическую информацию и

т.п. В некоторых воплощениях устройство для обработки данных может объединять динамическую информацию со статической информацией для генерирования временного идентификатора. За счет добавления динамической информации к статической информации вся информация последовательности может быть изменена за счет изменения небольшого элемента. Кроме того, хеш объединенной динамической информации и статической информации может отличаться от хеша только статической информации, без необходимости в изменении всего массива данных.

В некоторых воплощениях каждое устройство для обработки данных, задействованное в системе связи, может генерировать временный идентификатор. Каждое задействованное устройство связи может отправлять свой сгенерированный временный идентификатор на сервер аутентификации, который может функционировать как хранилище сгенерированных в реальном времени временных идентификаторов. Например, каждое из первого устройства для обработки данных и второго устройства для обработки данных может генерировать временные идентификаторы и может отправлять сгенерированные временные идентификаторы друг другу и на сервер аутентификации. В некоторых воплощениях первое устройство для обработки данных может отправлять запрос на сервер аутентификации, который содержит временный идентификатор, принятый первым устройством для обработки данных от второго устройства для обработки данных, запрашивая аутентификацию сервером аутентификации временного идентификатора второго устройства для обработки данных. Третье устройство для обработки данных может сравнивать временные идентификаторы второго устройства для обработки данных, принятые от второго устройства для обработки данных и первого устройства для обработки данных. В ответ на определение того, что временные идентификаторы соответствуют друг другу, третье устройство для обработки данных может отправлять на первое устройство для обработки данных указание о положительном результате аутентификации второго устройства для обработки данных. В некоторых воплощениях указание о положительном результате аутентификации может быть передано третьим устройством для обработки данных с помощью способов, сконфигурированных для исключения атак "человек посередине". В различных воплощениях третье устройство для обработки данных может функционировать в качестве хранилища во множестве применений, включая, без ограничения, системы финансового обслуживания, системы обеспечения безопасности брокерской деятельности, системы ведения медицинских архивов, системы защищенной связи для бизнеса, правительства, разведки и т.п., системы общественных архивов (например, реестры огнестрельного оружия, реестры Служб регистрации транспортных средств и т.п.), системы голосования и среди устройств Интернета вещей.

В ответ на определение того, что временные идентификаторы не соответствуют друг другу, третье устройство для обработки данных может отправлять на первое устройство для обработки данных указание об отрицательном результате аутентификации второго устройства для обработки данных. В некоторых воплощениях указание об отрицательном результате аутентификации может быть передано третьим устройством для обработки данных с помощью способов, сконфигурированных для исключения атак "человек посередине".

В некоторых воплощениях сервер аутентификации также может генерировать временный идентификатор и отправлять временный идентификатор третьего устройства для обработки данных на первое и второе устройства для обработки данных, и первое и второе устройства для обработки данных могут сравнивать временный идентификатор третьего устройства для обработки данных и аутентифицировать для себя идентификатор третьего устройства для обработки данных.

В некоторых воплощениях третье устройство для обработки данных вместе со своим временным идентификатором или отдельно от своего временного идентификатора может отправлять инструкцию на другие устройства для обработки данных (например, первое и второе устройства для обработки данных) для генерирования нового временного идентификатора. В различных воплощениях каждое устройство для обработки данных, задействованное в системе связи, может периодически или апериодически генерировать новый временный идентификатор. Во время продолжающегося сеанса связи такие новые временные идентификаторы могут быть сгенерированы в достаточной мере до истечения срока действия одного или более текущих временных идентификаторов, обеспечивающих безопасность сеанса связи, чтобы позволить двум устройствам для обработки данных и третьему устройству для обработки данных совершить обмены и аутентификации новых временных идентификаторов, вследствие чего сеанс связи может продолжаться без перерыва и под защитой новых идентификаторов. В некоторых воплощениях каждый новый временный идентификатор может быть предназначен для однократного использования, вследствие чего каждое устройство для обработки данных, которое принимает временный идентификатор от другого устройства для обработки данных, может только один раз использовать (взаимодействовать, аутентифицировать, обрабатывать, хешировать и т.п.) временный идентификатор, после чего принятый временный идентификатор становится непригодным к использованию. Опять-таки, продолжительность действия может быть задана для каждого нового временного идентификатора в течение срока действия, который меньше периода времени, в течение которого злоумышленник может получить и использовать временный идентификатор.

Различные воплощения могут предусматривать быстрое восстановление безопасности после успешной атаки. В различных воплощениях успешная атака на сервер аутентификации или другое устрой-

ство, задействованное в системе, не поставит под угрозу безопасность системы на существенный период времени, поскольку любая просочившаяся учетная информация не имеет долгосрочной ценности для злоумышленника, поскольку срок ее действия истечет до того, как ее можно будет использовать. Таким образом, система аутентификации может не быть поставлена под угрозу при атаке на сервер аутентификации. В различных воплощениях предлагается система связи, которая является долговечной и устойчивой, и успешно работает в среде, в которой каждый компонент может быть успешно атакован и скомпрометирован.

В некоторых воплощениях первое устройство для обработки данных и второе устройство для обработки данных могут устанавливать доверительное взаимоотношение на основании ранее совместно использованного хеша данных (например, с помощью алгоритма хеширования, такого как MD5, SHA1 или SHA2). Ранее совместно использованный хеш данных может быть создан, например, с помощью алгоритма с сохраненным и совместно использованным одноразовым паролем, основанным на времени (например, RFC 6238 инженерного совета Интернета, временный одноразовый пароль (TOTP) и т.п.). Такой ранее совместно использованный хеш данных может храниться в запоминающем устройстве на первом устройстве для обработки данных и/или втором устройстве для обработки данных. В некоторых воплощениях второе устройство для обработки данных может инициировать сеанс, такой как сеанс осуществления информационной транзакции или сеанс связи, когда второе устройство для обработки данных принимает от первого устройства для обработки данных данные входа в систему, такие как имя пользователя и пароль, которые могут быть связаны с учетной записью или идентификатором сеанса. В таких воплощениях, хотя данные входа в систему могут использоваться для идентификации учетной записи или сеанса, данные входа в систему могут не использоваться в целях обеспечения безопасности связи или аутентификации любого устройства для обработки данных или пользователя.

В некоторых воплощениях первое устройство для обработки данных может генерировать временный идентификатор и отправлять временный идентификатор на второе устройство вместе с данными входа в систему или отдельно от данных входа в систему. Первое устройство для обработки данных может генерировать временный идентификатор на основании динамических и/или статических аспектов первого устройства для обработки данных или указанных аспектов, определенных им. В некоторых воплощениях динамические аспекты первого устройства для обработки данных могут включать аспекты первого устройства для обработки данных, которые изменяются относительно быстро, такие как время такта, состояние чипа, состояние регистра, информация, принятая или обнаруженная датчиком устройства для обработки данных (например, акселерометра, оптического датчика, датчика температуры, датчика влажности и т.п.), информация от устройства системы глобального позиционирования (GPS) или сигнал Wi-Fi, или любой другой источник данных, основанных на динамическом аспекте первого устройства для обработки данных. В некоторых воплощениях динамические аспекты, определенные первым устройством для обработки данных, могут включать изображение или видеозапись, зафиксированную камерой, звукозапись окружающих звуков, зафиксированную микрофоном, видеозапись со звуком, зафиксированную камерой и микрофоном, или любую другую информацию об окружающей среде или окружающих условиях первого устройства для обработки данных. В некоторых воплощениях динамические аспекты могут быть получены от других источников, которые случайно и часто меняются, таких как внешние датчики и внешние источники случайной информации.

Второе устройство для обработки данных может отправлять запрос на аутентификацию на третье устройство для обработки данных, которое может функционировать как сервер аутентификации или сертифицирующий орган.

В некоторых воплощениях запрос на аутентификацию может содержать временный идентификатор, сгенерированный первым устройством для обработки данных. В некоторых воплощениях сервер аутентификации может хранить временный идентификатор первого устройства для обработки данных.

На основании запроса на аутентификацию от второго устройства для обработки данных третье устройство для обработки данных может отправлять запрос на аутентификацию на первое устройство для обработки данных. В ответ на запрос на аутентификацию от третьего устройства для обработки данных первое устройство для обработки данных может отправлять временный идентификатор первого устройства для обработки данных на третье устройство для обработки данных. В некоторых воплощениях первое устройство для обработки данных может генерировать хеш временного идентификатора первого устройства для обработки данных и может отправлять сгенерированный хеш временного идентификатора первого устройства для обработки данных на третье устройство для обработки данных.

В некоторых воплощениях третье устройство для обработки данных может сравнивать временный идентификатор первого устройства для обработки данных, принятый от второго устройства для обработки данных, и временный идентификатор первого устройства для обработки данных, принятый от первого устройства для обработки данных. В ответ на определение того, что два принятых временных идентификатора соответствуют друг другу, третье устройство для обработки данных может отправлять указание о положительном результате аутентификации первого устройства для обработки данных на второе устройство для обработки данных. В ответ на определение того, что два принятых временных идентификатора не соответствуют друг другу, третье устройство для обработки данных может отправлять указание об

отрицательном результате аутентификации первого устройства для обработки данных на второе устройство для обработки данных.

В некоторых воплощениях третье устройство для обработки данных может вести журнал контроля успешных и безуспешных попыток входа в систему. В некоторых воплощениях журнал контроля может содержать метаданные, идентифицирующие, например, время каждой попытки, идентификаторы первого и второго устройств для обработки данных (и любых других задействованных устройств для обработки данных), частоту использования, частоту отрицательных результатов аутентификации и другие детали. Журнал контроля может использоваться для анализа рисков и может быть отображен и/или доступен через панель управления или другой механизм отправки сообщений. В различных воплощениях любое из задействованных устройств для обработки данных может вести журнал контроля. В некоторых воплощениях копии временных идентификаторов могут храниться как часть журнала контроля. Такие сохраненные временные идентификаторы могут не использоваться в целях аутентификации, но могут использоваться для идентификации задействованных устройств для обработки данных, а также для подтверждения участия в конкретной информационной транзакции конкретным устройством для обработки данных. В некоторых воплощениях информация, хранящаяся в журнале контроля, может использоваться для идентификации, например, устройства для обработки данных, которое было целью атаки, осуществленной некоторым образом.

В различных воплощениях предлагается система, которая может аутентифицировать идентификатор устройства для обработки данных в системе связи на основании временной и/или динамической информации каждого устройства для обработки данных, в отличие от текущей парадигмы общих секретов и статической информации. В различных воплощениях задействованное устройство для обработки данных может аутентифицировать идентификатор второго устройства для обработки данных с помощью эфемерного временного идентификатора, который может быть принят от второго устройства для обработки данных и от третьего устройства для обработки данных (например, сервера аутентификации). Различные воплощения отличаются от текущей парадигмы безопасности, которая основана на сохранении в секрете статического фрагмента информации, такого как статический сертификат. Поскольку временный идентификатор каждого устройства для обработки данных часто меняется, и каждое устройство для обработки данных периодически (или апериодически) находится на связи с другими устройствами для обработки данных, отправляющими и/или принимающими новые временные идентификаторы, различные воплощения улучшают работу любой сети связи или любой системы электронной связи за счет повышения уровня безопасности связи. Нарушителю необходимо проникнуть в (минимум) три тракта связи - например, между первым и вторым устройствами для обработки данных, между первым и третьим устройствами для обработки данных и между вторым и третьим устройствами для обработки данных - одновременно и синхронно для компрометации связи между любыми двумя устройствами связи.

Различные воплощения могут быть реализованы с помощью множества устройств для обработки данных и/или сетей связи или систем без необходимости в существенных изменениях или переделках существующей в настоящее время инфраструктуры. Различные воплощения также улучшают работу любой сети связи за счет надежной аутентификации идентификатора задействованного устройства для обработки данных, не опираясь на статическую идентификационную информацию, такую как общий секрет, которая может быть уязвимой к атаке в результате доступа и/или копирования.

В различных воплощениях устройство для обработки данных, которое сконфигурировано для выполнения различных способов, может быть деавторизовано или заблокировано от доступа к системе в случае кражи или изготовления копии устройства для обработки данных.

Различные воплощения могут быть реализованы в пределах множества систем 150 связи, один пример которых изображен на фиг. 1А. Система 150 связи может содержать множество объектов, которые могут связываться с помощью сети связи, таких как сеть 154 IoT, юридическая фирма 156, военный подрядчик 158, субподрядчик 160, банк 162, объект 164 здравоохранения, объект 166 онлайн-торговли и телекоммуникационный объект 168. Каждый из объектов 154-168 может связываться с другим и находиться на связи между другими объектами. Каждый из объектов 154-168 также может связываться с сертифицирующим органом 152. Сертифицирующий орган 152 может включать одно или более устройств для обработки данных, сконфигурированных для выполнения операций, обеспечивающих аутентификацию идентификатора устройства для обработки данных, как подробнее описано ниже. Объекты 154-168 приведены исключительно в качестве примера, и сеть 150 связи может содержать широкий выбор объектов, включая объекты, которые могут управлять медицинскими архивами, защищенной связью (например, для бизнеса или правительственного учреждения), общественными архивами, системами голосования, финансовыми службами, системами обеспечения безопасности брокерской деятельности, связью IoT, коммерческими операциями и широким выбором подобного.

Различные воплощения могут быть реализованы в пределах множества систем 100 связи, один пример которых изображен на фиг. 1В. Как показано на фиг. 1А и 1В, элементы системы 100 связи могут использоваться в любом из объектов 154-168. Система 100 связи может содержать устройства 102, 104, 106 и 108 для обработки данных. В некоторых воплощениях устройства 102 и 104 для обработки данных могут включать устройство для обработки данных, непосредственно используемое пользователем, такое

как смартфон, портативный компьютер, настольный компьютер и т.п. Следует понимать, что пользователь может управлять более чем одним таким устройством для обработки данных, аналогичным устройствам 102 и 104 для обработки данных. В некоторых воплощениях устройства 102 и 104 для обработки данных могут включать одно или более устройств IoT. Неограничивающие примеры устройств IoT включают персональные или мобильные мультимедийные проигрыватели, игровые системы и контроллеры, "умные" телевизоры, телевизионные приставки, "умные" кухонные приборы, "умные" светильники и системы освещения, "умные" электросчетчики, "умные" системы отопления, вентиляции и кондиционирования воздуха (HVAC), "умные" термостаты, системы обеспечения безопасности здания, включающие дверные и оконные замки, развлекательные системы в транспортном средстве, системы мониторинга и диагностики в транспортном средстве, межмашинные устройства и аналогичные устройства, которые содержат программируемый процессор, запоминающее устройство и схему для установления каналов беспроводной связи и передачи/приема данных по каналам беспроводной связи. Устройства 102 и 104 для обработки данных также могут включать беспилотное, автономное, полуавтономное или роботизированное транспортное средство, способное к перемещению по земле, воде, воздуху или в космосе. Устройства 102 и 104 для обработки данных могут также включать "умное" огнестрельное оружие или другое оснащенное процессором оружие или оружейную систему.

В некоторых воплощениях устройства 106 и 108 для обработки данных могут включать оконечное устройство для обработки данных, такое как сервер. В некоторых воплощениях устройство 108 для обработки данных может связываться с системой 114 обеспечения электронной безопасности по линии 130 связи. В некоторых воплощениях устройства 106 и 108 для обработки данных (и возможно устройство 114 для обработки данных) могут управляться одним объектом. Например, объект 164 здравоохранения или телекоммуникационный объект 168 могут управлять одним или более из устройств 106, 108 и/или 114 для обработки данных. В некоторых воплощениях устройства 106, 108 и 114 для обработки данных могут управляться более чем одним объектом.

Каждое из устройств 102, 104, 106 и 108 для обработки данных и системы 114 обеспечения электронной безопасности может связываться с сетью 112 связи по соответствующей линии 120, 122, 124, 126, 128 и 130 связи. Линии 120, 122, 124, 126, 128 и 130 связи могут включать линии проводной или беспроводной связи и могут дополнительно включать дополнительные устройства для упрощения связи между устройствами 102, 104, 106 и 108 для обработки данных, системой 114 обеспечения электронной безопасности и сетью 112 связи. Примеры таких дополнительных устройств могут включать точки доступа, базовые станции, маршрутизаторы, шлюзы, устройства проводной и/или беспроводной связи, а также линии связи транспортной сети, которые могут включать оптоволоконные линии транспортной сети, микроволновые линии транспортной сети и другие подходящие линии связи.

В некоторых воплощениях устройство 106 для обработки данных может быть сконфигурировано для выполнения операций, связанных с информационными транзакциями во множестве контекстов, включая, без ограничения, ведение медицинских архивов, защищенную связь, системы ведения общественных архивов, системы голосования, системы финансового обслуживания, системы обеспечения безопасности брокерской деятельности как контроллер устройства IoT для выполнения коммерческой операции, а также в других контекстах. В некоторых воплощениях устройство 108 для обработки данных может быть сконфигурировано для выполнения операций, связанных с генерированием и/или получением временных идентификаторов, и аутентификации идентификатора устройства для обработки данных, такого как одно или более из устройств 102, 104 и 106 для обработки данных, как подробнее описано ниже.

В некоторых воплощениях система 114 обеспечения электронной безопасности может быть сконфигурирована для выполнения функций мониторинга сети или обеспечения безопасности сети, таких как система мониторинга сети, система записи вводимой с клавиатуры информации или другая аналогичная система. В некоторых воплощениях система 114 обеспечения электронной безопасности может обнаруживать неавторизованного пользователя или электронного злоумышленника, использующего или получающего доступ к сети 112 связи, и может отправлять указание на устройство 108 для обработки данных об обнаружении неавторизованного пользователя или электронного злоумышленника. В некоторых воплощениях система 114 обеспечения электронной безопасности может быть сконфигурирована для мониторинга и/или обнаружения неавторизованных попыток доступа к системе, запоминающему устройству, сетевому элементу или компоненту сетевого элемента со стороны иным образом авторизованного пользователя (например, "внутренняя" угроза). В некоторых воплощениях система 114 обеспечения электронной безопасности может быть сконфигурирована для приема команды или указания о том, что устройство для обработки данных должно быть деавторизовано от доступа к системе связи. Например, система 114 обеспечения электронной безопасности может представлять собой компонент или элемент сетевой системы авторизации, или системы отдела кадров, или системы, которая предоставляет список авторизованных пользователей системы связи, или другой аналогичной системы. В таких воплощениях система 114 обеспечения электронной безопасности может принимать команду или другое сообщение, указывающее, что авторизация устройства для обработки данных должна быть отменена или заблокирована. В некоторых воплощениях в ответ на прием указания о том, что был обнаружен неавторизованный пользователь или электронный злоумышленник, что должна быть отменена или заблокирована авториза-

ция устройства для обработки данных, или другого аналогичного указания, устройство 108 для обработки данных может отправлять инструкцию на одно или более из устройств 102, 104 и 106 для обработки данных для получения нового временного идентификатора, как подробнее описано ниже.

Сеть 112 связи может включать множество сетей связи, включая сети связи в пределах объекта или предприятия и внешние сети связи, публичные сети связи, и комбинации сетей, а также интерсети, включая Интернет. Сеть 112 связи может поддерживать связь с помощью одного или более протоколов проводной и беспроводной связи. Каждая из линий 120, 122, 124 и 126 связи может представлять собой двустороннюю линию проводной или беспроводной связи. Протоколы беспроводной связи могут включать одну или более технологий радиодоступа (RAT). Примеры беспроводных RAT включают Долговременное развитие 3GPP (LTE), технологию широкополосного доступа в микроволновом диапазоне (WiMAX), множественный доступ с кодовым разделением (CDMA), множественный доступ с временным разделением (TDMA), широкополосный CDMA (WCDMA), глобальную систему мобильной связи (GSM) и другие RAT. Примеры RAT также могут включать Wi-Fi, Bluetooth, Zigbee, LTE в нелицензируемом спектре (LTE-U), доступ на базе лицензируемой полосы частот (LAA) и MuLTEfire (система, которая использует LTE на нелицензируемой полосе несущих частот). Протоколы проводной связи могут использовать множество проводных сетей (например, Ethernet, ТВ кабель, телефонную связь, оптоволокно и другие формы физических сетевых подключений), которые могут использовать один или более протоколов проводной связи, таких как Ethernet, протокол точка-точка, высокоуровневый протокол управления каналом (HDLC), улучшенный протокол управления передачей данных (ADCCP) и протокол управления передачей/протокол Интернета (TCP/IP).

Хотя линии 120, 122 и 124 связи изображены как отдельные линии, каждая из этих линий связи может содержать множество проводных или беспроводных линий, таких как множество частот или полос частот, каждая из которых может содержать множество логических каналов. Дополнительно, каждая из различных линий 120, 122 и 124 связи может использовать более одного протокола связи.

Устройство 108 для обработки данных может связываться с устройством 110 хранения данных, таким как запоминающее устройство, база данных, серверное устройство или другое устройство, способное хранить данные. В некоторых реализациях устройство 110 хранения данных может хранить журнал контроля и связанные метаданные.

Различные воплощения могут быть реализованы в пределах множества систем 180 связи, один пример которых изображен на фиг. 1С. Как показано на фиг. 1А-1С, элементы системы 150 связи могут использоваться в любом из объектов 154-168. Система 180 связи может содержать устройства 184, 186, 188, 190, 192, 194 и 196 для обработки данных. Устройства 190-196 для обработки данных могут содержать сетевые элементы, такие как файловые серверы, базы данных или другие аналогичные источники данных с доступом через сеть. Устройства 184 и 186 для обработки данных могут включать любую форму управляемого пользователем сетевого терминала и могут быть аналогичны устройствам 102 и 104 для обработки данных. Устройства 186-196 для обработки данных могут представлять собой элементы в сети 182 связи, доступ к которым может быть защищен устройством, сконфигурированным для защиты электронного доступа к сети 182 связи, таким как брандмауэр 198.

Традиционные реализации обеспечения безопасности связи, такие как брандмауэр 198, могут защищать сеть 182 от атак или использования внешним устройством, таким как устройство 184 для обработки данных. Однако брандмауэр 198 может не защитить сеть 182 от атак или использования устройством, которое находится внутри брандмауэра 198, таким как устройство 186 для обработки данных.

Различные воплощения могут включать устройство 188 для обработки данных (которое может быть аналогичным третьему устройству 108 для обработки данных), которое может быть сконфигурировано для выполнения операций, связанных с генерированием и/или получением временных идентификаторов и аутентификацией идентификатора устройства для обработки данных, такого как одно или более из устройств 184, 186, 190, 192, 194 и 196 для обработки данных.

В различных воплощениях, хотя брандмауэр 198 может использоваться для выполнения сетевых операций, таких как мониторинг трафика, функции шлюза, маршрутизация и других аналогичных функций, брандмауэр 198 может не выполнять функцию обеспечения безопасности или функцию аутентификации устройств, таких как устройства 184 и 186 для обработки данных. Скорее, в системе 180 связи устройства 184 и 186 для обработки данных могут связываться с устройством 188 для обработки данных и/или друг с другом, обеспечивая аутентификацию идентификатора каждого из устройств 184 и 186 для обработки данных, а также в некоторых воплощениях идентификатора устройства 188 для обработки данных. Аналогично, хотя система 180 связи может использовать входные данные, принятые на устройстве 184 или 186 для обработки данных, такие как имя пользователя и пароль, для идентификации предполагаемого пользователя или в качестве указателя на учетную запись пользователя, система 180 связи может не использовать учетные данные, такие как имя пользователя и пароль, в целях обеспечения безопасности или в целях аутентификации. Скорее, система 180 связи может аутентифицировать идентификатор устройств 184 и 186 для обработки данных на основании временной и/или динамической информации каждого устройства для обработки данных, что подробнее описано ниже.

На фиг. 2 показана блок-схема компонентов устройства 200 для обработки данных, подходящего

для реализации различных воплощений. Как показано на фиг. 1 и 2, в различных воплощениях устройство 200 для обработки данных может быть аналогично устройствам 102, 104, 106 и 108 для обработки данных.

Устройство 200 для обработки данных может содержать процессор. Процессор 202 может быть сконфигурирован с выполняемыми процессором инструкциями для выполнения операций различных воплощений; может представлять собой специализированный процессор, такой как процессор модема, сконфигурированный с выполняемыми процессором инструкциями для выполнения операций различных воплощений в дополнение к основной функции; может представлять собой выделенную аппаратную (т.е. "программно-аппаратную") схему, сконфигурированную для выполнения операций различных воплощений, или комбинацию выделенного аппаратного обеспечения/программно-аппаратного обеспечения и программируемого процессора.

Процессор 202 может быть соединен с запоминающим устройством 204, которое может представлять собой постоянный машиночитаемый носитель, на котором хранятся выполняемые процессором инструкции. В запоминающем устройстве 204 может храниться операционная система, а также пользовательское прикладное программное обеспечение и выполняемые инструкции. В запоминающем устройстве 204 также могут храниться данные приложения, такие как структура данных массива. Запоминающее устройство 204 может содержать одну или более кеш-памятей, постоянное запоминающее устройство (ROM), оперативное запоминающее устройство (RAM), электрически стираемое программируемое ROM (EEPROM), статическое RAM (SRAM), динамическое RAM (DRAM) или другие типы запоминающего устройства. Процессор 202 может считывать информацию с запоминающего устройства 204 и записывать информацию на него. В запоминающем устройстве 204 также могут храниться инструкции, связанные с одним или более стеков протоколов. Стек протоколов обычно содержит выполняемые компьютером инструкции для обеспечения связи с помощью протокола радиодоступа или протокола связи.

Процессор 202 также может связываться с множеством модулей для блоков, сконфигурированных для выполнения множества операций, что подробнее описано ниже. Например, процессор 202 может связываться с интерфейсом 206 связи, модулем 208 аутентификации, модулем 210 хеширования, модулем 212 генерирования временного идентификатора, модулем 214 хранения хеша и модулем 216 обеспечения транзакции. Модули/блоки 206-216 могут быть реализованы на устройстве 200 для обработки данных в программном обеспечении и аппаратном обеспечении или в комбинации аппаратного обеспечения и программного обеспечения. Программно-аппаратное обеспечение, чип, система на чипе (SOC), выделенная аппаратная (т.е. "программно-аппаратная") схема сконфигурированы для выполнения операций различных воплощений или представляют собой комбинацию выделенного аппаратного обеспечения/программно-аппаратного обеспечения и программируемого процессора. Процессор 202, запоминающее устройство 204 и различные модули/блоки 206-216 могут связываться друг с другом по шине связи или любой другой схеме или интерфейсу связи.

Интерфейс 206 связи может содержать сетевой интерфейс, который может обеспечивать связь с сетью связи (например, сетью 112 связи). Интерфейс 206 связи может содержать один или более входных/выходных (I/O) портов, посредством которых может быть обеспечено соединение, такое как Ethernet-соединение, оптоволоконное соединение, соединение через широкополосный кабель, соединение через телефонную линию или другие типы соединения для проводной связи. Интерфейс 206 связи также может содержать блок радиосвязи, который может обеспечивать радиочастотную связь.

Модуль 208 аутентификации может обеспечивать связь или находиться на связи с одним или более устройствами ввода для получения ввода от пользователя для входа в систему на устройстве 200 для обработки данных. Устройства ввода могут включать одну или более кнопок, ползунков, сенсорных панелей, клавиатур, биометрических устройств ввода, камер, устройств считывания отпечатков пальцев и других аналогичных устройств ввода.

Модуль 212 генерирования временного идентификатора может генерировать временный идентификатор для устройства 200 для обработки данных. Временный идентификатор может быть основан на одном или более динамических аспектах устройства 200 для обработки данных, отдельно или в комбинации с другой динамической или статической информацией. Динамические аспекты устройства 200 для обработки данных могут включать аспекты первого устройства для обработки данных, которые меняются относительно быстро, такие как время такта, состояние чипа, состояние регистра, или любой другой источник данных, основанных на динамическом аспекте первого устройства для обработки данных.

Модуль 210 хеширования может генерировать хеш временного идентификатора, который сгенерирован модулем 212 генерирования временного идентификатора. Модуль 214 хранения хеша может содержать запоминающее устройство или может связываться с запоминающим устройством 204 для сохранения временного идентификатора, сгенерированного модулем 212 генерирования временного идентификатора, и/или хеша временного идентификатора, сгенерированного модулем 210 хеширования.

Модуль 216 обеспечения транзакции может обеспечивать связь, связанную с транзакцией (а также другие связи), с другим устройством для обработки данных (например, между устройством 102 для обработки данных и устройством 106 для обработки данных). В некоторых реализациях модуль 216 обеспечения транзакции может содержать аппаратное обеспечение и/или программное обеспечение, сконфи-

гурированное для обеспечения оптимизированной связи и/или процесса транзакции с сервером транзакций. В некоторых реализациях модуль обеспечения транзакции может содержать аппаратное обеспечение и/или программное обеспечение, сконфигурированное для обеспечения оптимизированной связи, связанной с выделенным поставщиком услуг, таких как так называемая услуга "за 1 щелчок", или другой оптимизированной связи/процесса транзакции.

На фиг. 3A и 3B показан осуществляемый системой способ 300 аутентификации первого устройства для обработки данных (например, устройства 102, 104, 184, 186 и 200 для обработки данных, показанного на фиг. 1B-2) относительно второго устройства для обработки данных (например, устройства 106, 190-196 и 200 для обработки данных, показанного на фиг. 1B-2), и наоборот посредством взаимодействия с третьим устройством для обработки данных (например, 108, 188 и 200 на фиг. 1B-2) согласно некоторым воплощениям. На фиг. 3C показана блок-схема способа 300a операций, выполняемых первым устройством для обработки данных как часть способа 300. На фиг. 3D показана блок-схема способа 300b операций, выполняемых вторым устройством для обработки данных как часть способа 300. На фиг. 3E показана блок-схема способа 300c операций, выполняемых третьим устройством для обработки данных как часть способа 300. Как показано на фиг. 1A-3E, способ 300 может быть реализован процессором (например, процессором 202 и/или подобным) первого устройства для обработки данных (т.е. процессором устройства), процессором второго устройства для обработки данных и процессором третьего устройства для обработки данных.

В различных воплощениях перед осуществлением способа 300 или в качестве его части первое устройство для обработки данных (например, устройство 102 или 104 для обработки данных) и второе устройство для обработки данных (например, устройство 106 для обработки данных) могут устанавливать связи с третьим устройством для обработки данных (например, устройством 108 для обработки данных), которое может в некоторых воплощениях функционировать как сервер аутентификации. В различных воплощениях первое устройство для обработки данных и второе устройство для обработки данных могут быть сконфигурированы (например, для инициализации, настройки, установки и т.п.) с одним или более модулями, обеспечивающими выполнение каждым устройством для обработки данных операций способа 300 (например, модули 206-216).

В некоторых воплощениях установление связи с третьим устройством для обработки данных может включать определение и/или согласование тракта связи между третьим устройством для обработки данных и первым/вторым устройством для обработки данных. В некоторых воплощениях каждое из первого и второго устройств для обработки данных может согласовывать или определять тракт связи с третьим устройство для обработки данных, который отличается в одном или более аспектах. Например, каждая пара устройств для обработки данных может использовать отличающийся способ или протокол шифрования, протокол или приложение связи (например, язык гипертекстовой разметки (HTML), текстовое сообщение службы коротких сообщений (SMS)) и т п. В различных воплощениях пользователь может устанавливать множество связей с множеством серверов аутентификации без ограничения.

Различные воплощения могут обеспечивать защиту от вторжения и компрометации связи между любыми двумя из первого устройства для обработки данных, второго устройства для обработки данных и третьего устройства для обработки данных. Например, злоумышленник, осуществляющий атаку "человек посередине" (MITM), может тайно передавать сообщения между двумя сетевыми устройствами и может осуществлять мониторинг и/или изменять эти сообщения. В различных воплощениях требуется, чтобы злоумышленник одновременно скомпрометировал три тракта связи практически одновременно: первый тракт связи между первым устройством для обработки данных и вторым устройством для обработки данных, второй тракт связи между вторым устройством для обработки данных и третьим устройством для обработки данных и третий тракт связи между третьим устройством для обработки данных и первым устройством для обработки данных. Поскольку временные идентификаторы являются динамическими и часто меняются, злоумышленнику необходимо украсть или перехватить и очень быстро расшифровать временные идентификаторы, отправленные по указанным трем трактам связи. Потенциальная уязвимость исключается за счет короткого срока действия разной аутентифицирующей информации, передаваемой между тремя устройствами для обработки данных по трем отдельным трактам связи.

В блоке 302 способа 300 и 300a процессор первого устройства для обработки данных (например, устройства 102 или 104 для обработки данных) может получать первый временный идентификатор. В некоторых воплощениях процессор первого устройства для обработки данных может получать первый временный идентификатор за счет генерирования первого временного идентификатора (например, операция 302a). В некоторых воплощениях процессор первого устройства для обработки данных может получать сгенерированный первый временный идентификатор от третьего устройства для обработки данных (например, устройства 108 для обработки данных) (например, операция 302b). В некоторых воплощениях процессор третьего устройства для обработки данных может отправлять сгенерированный первый временный идентификатор на первое устройство для обработки данных (например, третье устройство для обработки данных может отправлять сгенерированный временный идентификатор на первое устройство для обработки данных без запроса от первого устройства для обработки данных). В некоторых воплощениях процессор первого устройства для обработки данных может принимать первый временный

идентификатор от третьего устройства для обработки данных. Например, первое устройство для обработки данных может отправлять запрос на предоставление временного идентификатора на третье устройство для обработки данных, и третье устройство для обработки данных может отправлять временный идентификатор на первое устройство для обработки данных в ответ на запрос.

В блоке 304 способа 300 и 300b процессор второго устройства для обработки данных (например, устройства 106 для обработки данных) может генерировать второй временный идентификатор (например, операция 304a). В некоторых воплощениях процессор второго устройства для обработки данных может получать первый временный идентификатор за счет генерирования второго временного идентификатора. В некоторых воплощениях процессор второго устройства для обработки данных может получать второй временный идентификатор от третьего устройства для обработки данных (например, операция 304b). В некоторых воплощениях процессор третьего устройства для обработки данных может отправлять второй временный идентификатор на второе устройство для обработки данных. В некоторых воплощениях процессор второго устройства для обработки данных может принимать сгенерированный второй временный идентификатор от третьего устройства для обработки данных.

В опциональном блоке 306 способа 300 и 300c процессор третьего устройства для обработки данных (например, устройства 108 для обработки данных) может генерировать третий временный идентификатор.

В блоке 308 способа 300 и 300a процессор первого устройства для обработки данных может отправлять первый временный идентификатор на второе устройство для обработки данных и третье устройство для обработки данных. Передача первого временного идентификатора на второе устройство для обработки данных может осуществляться по открытой линии связи, такой как линия связи, которая находится в процессе установления между первым устройством для обработки данных и вторым устройством для обработки данных. В некоторых воплощениях связь может быть зашифрована и, следовательно, передача может быть выполнена после обмена первоначальным ключом шифрования. В некоторых воплощениях линия связи может быть открытой (т.е. незашифрованной), вследствие чего устройства для обработки данных могут аутентифицировать друг друга посредством различных воплощений перед обменом ключами шифрования. Передача первого временного идентификатора на третье устройство для обработки данных может осуществляться по другой линии связи, которая может зашифрована или не зашифрована. В некоторых воплощениях эта передача может осуществляться посредством публичной сети, такой как Интернет. В некоторых воплощениях эта передача может осуществляться по частной или выделенной линии связи.

В блоке 310 способа 300 и 300b процессор второго устройства для обработки данных может отправлять второй временный идентификатор на первое устройство для обработки данных и третье устройство для обработки данных. Передача второго временного идентификатора на первое устройство для обработки данных может осуществляться по любой открытой линии связи, такой как линия связи, которая находится в процессе установления между первым устройством для обработки данных и вторым устройством для обработки данных, посредством которой второе устройство для обработки данных принимает первый временный идентификатор. В некоторых воплощениях связь может быть зашифрована и, следовательно, передача может быть выполнена после обмена первоначальным ключом шифрования. В некоторых воплощениях линия связи может быть открытой (т.е. незашифрованной), вследствие чего устройства для обработки данных могут аутентифицировать друг друга посредством различных воплощений перед обменом ключами шифрования. Передача второго временного идентификатора на третье устройство для обработки данных может осуществляться по другой линии связи, которая может зашифрована или не зашифрована. В некоторых воплощениях эта передача может осуществляться посредством публичной сети, такой как Интернет. В некоторых воплощениях эта передача может осуществляться по частной или выделенной линии связи.

В опциональном блоке 312 способа 300 и 300c процессор третьего устройства для обработки данных может отправлять третий временный идентификатор на первое устройство для обработки данных и второе устройство для обработки данных. Передача третьего временного идентификатора на первое и второе устройства для обработки данных может осуществляться по тем же линиям связи, по которым третье устройство для обработки данных приняло первый и второй временные идентификаторы. Такие линии связи могут быть зашифрованы или не зашифрованы. В некоторых воплощениях эта передача может осуществляться посредством публичной сети, такой как Интернет. В некоторых воплощениях эта передача может осуществляться по частной или выделенной линии связи.

В блоке 314 способа 300 и 300a процессор первого устройства для обработки данных может отправлять запрос на аутентификацию, содержащий второй временный идентификатор, на третье устройство для обработки данных. В некоторых воплощениях первое устройство для обработки данных может отправлять запрос на аутентификацию автоматически, например, в фоновом режиме. В некоторых воплощениях первое устройство для обработки данных может отправлять запрос на аутентификацию в ответ на команду. В некоторых воплощениях запрос на аутентификацию может содержать небольшой фрагмент информации, который может храниться на первом устройстве для обработки данных, такой как текст, изображение, биометрическая информация или другая легко персонализируемая информация. В

некоторых воплощениях первое устройство для обработки данных может содержать небольшой фрагмент информации в запросе на аутентификацию или с ним.

В блоке 316 способа 300 и 300b процессор второго устройства для обработки данных может отправлять запрос на аутентификацию, содержащий первый временный идентификатор, на третье устройство для обработки данных.

В блоке 318 определения способа 300 и 300c процессор третьего устройства для обработки данных может определять, соответствует ли второй временный идентификатор от первого устройства для обработки данных второму временному идентификатору от второго устройства для обработки данных. В некоторых воплощениях третье устройство для обработки данных может выполнять эту операцию путем прямого сравнения двух принятых временных идентификаторов (например, вычитания и проверки на наличие остатка). В некоторых воплощениях третье устройство для обработки данных может выполнять эту операцию путем выполнения хеш-функции на одном или обоих принятых временных идентификаторах и определения, соответствуют ли друг друга эти два идентификатора путем сравнения результатов хеш-функции (хеш-функций).

В ответ на определение того, что второй временный идентификатор от первого устройства для обработки данных не соответствует второму временному идентификатору от второго устройства для обработки данных (т.е. блок определения 318="Нет"), процессор третьего устройства для обработки данных может отправлять указание об отрицательном результате аутентификации второго устройства для обработки данных на первое устройство для обработки данных и/или второе устройство для обработки данных в блоке 322.

В ответ на определение того, что второй временный идентификатор от первого устройства для обработки данных соответствует второму временному идентификатору от второго устройства для обработки данных (т.е. блок определения 318="Да"), процессор третьего устройства для обработки данных может отправлять указание о положительном результате аутентификации второго устройства для обработки данных на первое устройство для обработки данных и/или второе устройство для обработки данных в блоке 326.

В блоке 320 определения способа 300 и 300c процессор третьего устройства для обработки данных может определять, соответствует ли первый временный идентификатор от второго устройства для обработки данных первому временному идентификатору от первого устройства для обработки данных.

В ответ на определение того, что первый временный идентификатор от второго устройства для обработки данных не соответствует первому временному идентификатору от первого устройства для обработки данных (т.е. блок определения 320="Нет"), процессор третьего устройства для обработки данных может отправлять указание об отрицательном результате аутентификации первого устройства для обработки данных на первое устройство для обработки данных и/или второе устройство для обработки данных в блоке 324.

В ответ на определение того, что первый временный идентификатор от второго устройства для обработки данных соответствует первому временному идентификатору от первого устройства для обработки данных (т.е. блок определения 320="Да"), процессор третьего устройства для обработки данных может отправлять указание о положительном результате аутентификации второго устройства для обработки данных на первое устройство для обработки данных и/или второе устройство для обработки данных в блоке 328.

В некоторых реализациях указания об отрицательном результате аутентификации или положительном результате аутентификации могут содержать очень короткое сообщение или структуру данных, а в некоторых реализациях указание может содержать один бит, такой как 0 или 1, указывающий на отрицательный результат аутентификации или положительный результат аутентификации соответственно.

После операций блоков 326 и/или 328 способов 300 и 300c процессор третьего устройства для обработки данных может отправлять инструкцию на первое устройство для обработки данных и второе устройство для обработки данных на получение новых временных идентификаторов в блоке 330. В некоторых воплощениях инструкция может включать инструкцию на генерирование нового временного идентификатора на первом и втором устройствах для обработки данных соответственно. В некоторых воплощениях инструкция может включать инструкцию для каждого из первого и второго устройств для обработки данных соответственно на получение нового временного идентификатора от третьего устройства для обработки данных. В некоторых воплощениях третье устройство для обработки данных может генерировать и отправлять новый временный идентификатор для каждого из первого и второго устройств для обработки данных без запроса от первого или второго устройств для обработки данных.

Процессоры первого, второго и третьего устройств для обработки данных могут затем выполнять операции блоков 302, 304 и 306 способов 300, 300a, 300b и 300c соответственно. Первое, второе и третье устройства для обработки данных могут периодически повторять операции способов 300, 300a, 300b и 300c для выполнения непрерывной, периодической фоновой аутентификации других устройств для обработки данных. В некоторых воплощениях процессоры первого, второго и третьего устройств для обработки данных могут периодически повторять операции способов 300, 300a, 300b и 300c с инструкцией или другим сообщением от другого из первого, второго и третьего устройств для обработки данных или

без них. За счет использования динамической системы аутентификации устройств способы 300, 300a, 300b и 300c существенно уменьшают вероятность перехвата любого из временных идентификаторов и их использования, чтобы выдать себя за одно из устройств для обработки данных.

В некоторых воплощениях третье устройство для обработки данных может выполнять операции блока 330 и 300c в случае отрицательного результата аутентификации первого устройства для обработки данных и/или второго устройства 332 для обработки данных. Например, третье устройство для обработки данных может отвечать на отрицательный результат аутентификации устройства для обработки данных в виде указания о компрометации или попытке компрометации задействованного устройства для обработки данных или системы. В различных воплощениях в качестве ответа на возможный взлом или фактический взлом связи системы третье устройство для обработки данных может отдавать инструкцию всем задействованным устройствам для обработки данных на получение новых временных идентификаторов. Поскольку только те устройства для обработки данных, которые сконфигурированы для участия в системе, могут получить новый временный идентификатор, устройства для обработки данных, которые не сконфигурированы таким образом - такие как кибернетические злоумышленники и другие нарушители - не смогут получить новый временный идентификатор и будут эффективно заблокированы от дальнейшей связи с использованием системы.

В некоторых воплощениях процессоры первого, второго и третьего устройств для обработки данных могут повторять свои соответствующие операции с частотой, которая меньше, чем определенное время, необходимое злоумышленнику для получения и использования первого и/или второго временных идентификаторов.

Например, в некоторых воплощениях срок действия первого, второго и/или третьего временных идентификаторов ("сроки действия") может быть задан более коротким, чем время, которое требуется злоумышленнику для получения и использования одного или более временных идентификаторов. В некоторых воплощениях процессор первого, второго и/или третьего устройств для обработки данных может получать новый временный идентификатор в ответ на определение того, что срок действия соответствующего первого и/или второго временного идентификатора истек. В некоторых воплощениях процессор третьего устройства для обработки данных может генерировать новый временный идентификатор для первого, второго и/или третьего устройств для обработки данных в ответ на определение того, что срок действия соответствующего первого и/или второго временного идентификатора истек.

На фиг. 3C показана блок-схема способа 300a операций, выполняемых первым устройством для обработки данных как часть способа 300. Как показано на фиг. 1A-3E, способ 300a может быть реализован процессором (например, процессором 202 и/или подобным). В блоках 302, 308 и 314 процессор первого устройства для обработки данных может выполнять операции аналогично пронумерованных блоков способа 300.

В блоке 333 определения процессор первого устройства для обработки данных может определять, принимается или было принято указание о положительном результате аутентификации или указание об отрицательном результате аутентификации от третьего устройства для обработки данных. В некоторых опциональных воплощениях процессор также может определять, что никакое указание не принято от третьего устройства для обработки данных.

В ответ на определение того, что указание об отрицательном результате аутентификации принимается или было принято (т.е. блок определения 333="Отрицательный результат"), или опционально в ответ на определение того, что никакое указание не было принято (блок определения 333="Нет указания"), процессор первого устройства для обработки данных может сохранять указание об отрицательном результате аутентификации в блоке 334.

В блоке 336 процессор первого устройства для обработки данных может выполнять действие по обеспечению безопасности. Например, процессор первого устройства для обработки данных может прекращать выполнение информационной транзакции со вторым устройством для обработки данных. Процессор первого устройства для обработки данных также может блокировать дальнейшую связь со вторым устройством для обработки данных.

В ответ на определение того, что указание о положительном результате аутентификации принимается или было принято (т.е. блок 333 определения="Положительный результат"), процессор первого устройства для обработки данных может сохранять указание о положительном результате аутентификации в блоке 338.

В блоке 340 процессор первого устройства для обработки данных может выполнять информационную транзакцию со вторым устройством для обработки данных. Процессор первого устройства для обработки данных может затем получать новый временный идентификатор в блоке 302. Например, процессор первого устройства для обработки данных может определять, что срок действия временного идентификатора истек, и в ответ на определение того, что срок действия временного идентификатора истек, процессор первого устройства для обработки данных может получать новый временный идентификатор в блоке 302.

В опциональном блоке 342 процессор первого устройства для обработки данных может принимать инструкцию от третьего устройства для обработки данных на получение нового временного идентифика-

тора. Процессор первого устройства для обработки данных затем может выполнять операции блока 302.

На фиг. 3D показана блок-схема способа 300b операций, выполняемых вторым устройством для обработки данных как часть способа 300. Как показано на фиг. 1A-3E, способ 300b может быть реализован процессором (например, процессором 202 и/или подобным). В блоках 304, 310 и 316 процессор второго устройства для обработки данных может выполнять операции аналогично пронумерованных блоков способа 300.

В блоке 344 определения процессор второго устройства для обработки данных может определять, принимается или было принято указание о положительном результате аутентификации или указание об отрицательном результате аутентификации от третьего устройства для обработки данных. В некоторых опциональных воплощениях процессор также может определять, что никакое указание не принято от третьего устройства для обработки данных.

В ответ на определение того, что указание об отрицательном результате аутентификации принимается или было принято (т.е. блок определения 344="Отрицательный результат"), или опционально в ответ на определение того, что никакое указание не было принято (блок определения 344="Нет указания"), процессор второго устройства для обработки данных может сохранять указание об отрицательном результате аутентификации в блоке 346.

В блоке 348 процессор второго устройства для обработки данных может выполнять действие по обеспечению безопасности. Например, процессор второго устройства для обработки данных может прекращать выполнение информационной транзакции с первым устройством для обработки данных. Процессор второго устройства для обработки данных также может блокировать дальнейшую связь с первым устройством для обработки данных.

В ответ на определение того, что процессор принимает указание о положительном результате аутентификации (т.е. блок 344 определения="Положительный результат"), процессор второго устройства для обработки данных может сохранять указание о положительном результате аутентификации в блоке 350.

В блоке 352 процессор второго устройства для обработки данных может выполнять информационную транзакцию с первым устройством для обработки данных.

Процессор второго устройства для обработки данных может затем получать новый временный идентификатор в блоке 304. Например, процессор второго устройства для обработки данных может определять, что срок действия второго временного идентификатора истек, и в ответ на определение того, что срок действия второго временного идентификатора истек, процессор второго устройства для обработки данных может получать новый временный идентификатор в блоке 304.

В опциональном блоке 354 процессор второго устройства для обработки данных может принимать инструкцию от третьего устройства для обработки данных на получение нового временного идентификатора. Процессор второго устройства для обработки данных затем может выполнять операции блока 304.

На фиг. 3E показана блок-схема способа 300c операций, выполняемых третьим устройством для обработки данных как часть способа 300. Как показано на фиг. 1A-3E, способ 300c может быть реализован процессором (например, процессором 202 и/или подобным). В блоках 306-330 процессор третьего устройства для обработки данных может выполнять операции аналогично пронумерованных блоков способа 300.

В блоке 360 процессор третьего устройства для обработки данных может принимать запрос на аутентификацию от первого устройства для обработки данных. В блоке 318 определения процессор третьего устройства для обработки данных может определять, соответствует ли второй временный идентификатор от первого устройства для обработки данных второму временному идентификатору от второго устройства для обработки данных, как описано выше.

В блоке 362 процессор третьего устройства для обработки данных может принимать запрос на аутентификацию от второго устройства для обработки данных. В блоке 320 определения процессор третьего устройства для обработки данных может определять, соответствует ли первый временный идентификатор от второго устройства для обработки данных первому временному идентификатору от первого устройства для обработки данных, как описано выше.

На фиг. 4A показан способ 400 аутентификации устройства для обработки данных и авторизации информационной транзакции первого устройства для обработки данных (например, устройства 102, 104, 184, 186 и 200 для обработки данных, показанного на фиг. 1B-2) со вторым устройством для обработки данных (например, устройством 106, 190-196 и 200 для обработки данных, показанным на фиг. 1B-2) и наоборот посредством взаимодействия с третьим устройством для обработки данных (например, 108, 188 и 200 на фиг. 1B-2) согласно некоторым воплощениям. На фиг. 4B показана блок-схема способа 400a операций, выполняемых первым устройством для обработки данных как часть способа 400. На фиг. 4C показана блок-схема способа 400b операций, выполняемых вторым устройством для обработки данных как часть способа 400. На фиг. 4D показана блок-схема способа 400c операций, выполняемых третьим устройством для обработки данных как часть способа 400. Как показано на фиг. 1A-4D, способ 400 может быть реализован процессором (например, процессором 202 и/или подобным) устройства для обработки данных (т.е. процессором устройства).

В опциональном блоке 402 процессор первого устройства для обработки данных (например, устройства 102 и 104 для обработки данных) может отправлять информацию, идентифицирующую учетную запись пользователя, на второе устройство для обработки данных (например, устройство 106 для обработки данных).

В опциональном блоке 404 процессор второго устройства для обработки данных может подтверждать соответствие идентифицирующей информации учетной записи первого устройства для обработки данных. В некоторых воплощениях второе устройство для обработки данных может отправлять сообщение, указывающее подтверждение, на первое устройство для обработки данных.

В некоторых воплощениях идентифицирующая информация, используемая в блоке 402, может содержать ранее использованный временный идентификатор, используемый при связи со вторым устройством для обработки данных, такой как наиболее недавно использованный или последний использованный временный идентификатор, который был использован для связи между первым и вторым устройствами для обработки данных. В таких воплощениях ранее использованный временный идентификатор может использоваться исключительно в целях первоначальной идентификации и может не использоваться для аутентификации идентификатора первого устройства связи. В некоторых воплощениях использование ранее использованного временного идентификатора может обеспечивать улучшенную идентификацию (но не аутентификацию) предполагаемого идентификатора первого устройства для обработки данных. В некоторых воплощениях, поскольку второе устройство для обработки данных ранее приняло ранее использованный временный идентификатор, ранее использованный временный идентификатор может использоваться для двухфакторной (или многофакторной) идентификации первого устройства для обработки данных. Кроме того, поскольку ранее использованный временный идентификатор может не отображаться или не предоставляться пользователю первого устройства для обработки данных в силу чрезвычайно большой сложности его получения от первого устройства для обработки данных, использование ранее использованного временного идентификатора для первоначальной идентификации первого устройства для обработки данных может быть более надежным, чем использование имени пользователя и пароля, которые можно увидеть, например, взглянув на дисплей первого существующего устройства. В некоторых воплощениях ранее использованный временный идентификатор также может использоваться для быстрого восстановления состояния предыдущей связи (например, просматриваемого сайта, прочитываемого сообщения, просматриваемого изображения и т.п.). В некоторых воплощениях такая информация о состоянии может быть закодирована во временном идентификаторе.

В некоторых воплощениях идентифицирующая информация может содержать традиционные имя пользователя и пароль или другую обычную идентифицирующую информацию. В таких воплощениях идентифицирующая информация может использоваться исключительно в целях идентификации предполагаемого идентификатора первого устройства связи, но не для аутентификации первого устройства для обработки данных или второго устройства для обработки данных.

В блоке 406 процессор первого устройства для обработки данных может отправлять запрос на второе устройство для обработки данных на выполнение информационной транзакции. В некоторых воплощениях информационная транзакция может включать предоставление информации в электронную службу медицинских архивов или службу общественных архивов, базу данных регистрации избирателей или систему голосования, для онлайн-покупки, банковской транзакции или другого аналогичного обмена информацией или электронной транзакции.

В блоке 408 процессор второго устройства для обработки данных может отправлять запрос на третье устройство для обработки данных на подтверждение идентификатора первого устройства для обработки данных.

В блоке 410 процессор второго устройства для обработки данных может отправлять запрос на предоставление временного идентификатора на первое устройство для обработки данных. В некоторых реализациях запрос может содержать инструкцию на генерирование или может запускать генерирование нового временного идентификатора первым устройством для обработки данных. В некоторых воплощениях запрос может содержать инструкцию на получение нового временного идентификатора от третьего устройства для обработки данных. Эта передача временного идентификатора может быть осуществлена посредством или с использованием любого из каналов связи и способов, описанных со ссылкой на способ 300.

В блоке 412 процессор первого устройства для обработки данных может отправлять временный идентификатор от первого устройства для обработки данных на второе устройство для обработки данных и на третье устройство для обработки данных. Эта передача временного идентификатора может быть осуществлена посредством или с использованием любого из каналов связи и способов, описанных со ссылкой на способ 300.

В блоке 414 второе устройство для обработки данных может отправлять временный идентификатор, принятый от первого устройства для обработки данных, на третье устройство для обработки данных. Третье устройство для обработки данных, таким образом, может принимать временный идентификатор, сгенерированный первым устройством для обработки данных, от первого устройства для обработки данных и по отдельному тракту связи временный идентификатор первого устройства для обработки данных

от второго устройства для обработки данных. Эта передача временного идентификатора может быть осуществлена посредством или с использованием любого из каналов связи и способов, описанных со ссылкой на способ 300.

В блоке 416 процессор третьего устройства для обработки данных может сравнивать временный идентификатор первого устройства для обработки данных, принятый от первого устройства для обработки данных, и временный идентификатор первого устройства для обработки данных, принятый от второго устройства для обработки данных.

В блоке 418 определения процессор третьего устройства для обработки данных может определять, соответствуют ли временные идентификаторы друг другу.

В ответ на определение того, что временные идентификаторы не соответствуют друг другу (т.е. блок определения 418="Нет"), процессор третьего устройства для обработки данных может отправлять указание об отрицательном результате подтверждения первого устройства для обработки данных в блоке 420. Это передача указания об отрицательном результате подтверждения может быть осуществлена посредством или с использованием любого из каналов связи и способов, описанных со ссылкой на способ 300 для аналогичных передач. В некоторых воплощениях процессор третьего устройства для обработки данных может отправлять уведомление об отрицательном результате на второе устройство для обработки данных. В некоторых воплощениях процессор третьего устройства для обработки данных может отправлять уведомление об отрицательном результате третьей стороне, такой как устройство для обработки данных специалиста по информационной безопасности.

В блоке 421 третье устройство для обработки данных может выполнять действие на основании отрицательного результата подтверждения первого устройства для обработки данных. В некоторых воплощениях процессор третьего устройства для обработки данных может отправлять уведомление об отрицательном результате на опубликованную электронную почту, которая связана с первым устройством для обработки данных для уведомления зарегистрированного пользователя первого устройства для обработки данных о возможной компрометации первого устройства для обработки данных. В некоторых воплощениях процессор третьего устройства для обработки данных может определять, претендует ли более одного устройства для обработки данных считаться первым устройством для обработки данных. Обнаружение более одного устройства для обработки данных, претендующего считаться первым устройством для обработки данных, может указывать, что первое устройство для обработки данных было скопировано или иным образом дублировано в некотором роде. В некоторых воплощениях, если процессор третьего устройства для обработки данных обнаруживает скопированное/дублированное устройство для обработки данных, третье устройство для обработки данных может отправлять предупредительный сигнал, деавторизовывать первое устройство для обработки данных от участия в системе, может не впускать первое устройство для обработки данных в систему и/или может отправлять команду на деактивацию первого устройства для обработки данных.

В ответ на определение того, что временные идентификаторы соответствуют друг другу (т.е. блок 418 определения="Да"), процессор третьего устройства для обработки данных может отправлять указание о положительном результате подтверждения первого устройства для обработки данных в блоке 422. Это передача указания о положительном результате подтверждения может быть осуществлена посредством или с использованием любого из каналов связи и способов, описанных со ссылкой на способ 300 для аналогичных передач. В некоторых воплощениях процессор третьего устройства для обработки данных может отправлять указание о положительном результате подтверждения на второе устройство для обработки данных и на первое устройство для обработки данных.

В различных воплощениях после подтверждения идентификатора первого устройства для обработки данных задействованные устройства для обработки данных могут выполнять операции по обеспечению аутентификации участия одного или более из задействованных устройств для обработки данных (например, первого устройства для обработки данных, второго устройства для обработки данных и т.д.). В некоторых воплощениях аутентификация участия одного или более из задействованных устройств для обработки данных может обеспечивать неопровержимость информационной транзакции. В некоторых воплощениях операции, обеспечивающие аутентификацию участия одного или более из задействованных устройств для обработки данных, могут выступать в качестве замены других традиционных операций по аутентификации участия устройства для обработки данных (или пользователя) в информационной транзакции, таких как получение подписи, требование ввода пароля или кода или требование дополнительного пользовательского взаимодействия (например, "нажатия" на кнопку подтверждения).

В блоке 424 процессор первого устройства для обработки данных может генерировать текстовую строку и может генерировать зашифрованную версию текстовой строки.

В блоке 426 первое устройство для обработки данных может отправлять сгенерированную нешифрованную текстовую строку на второе устройство для обработки данных. Это передача может быть осуществлена посредством или с использованием любого из каналов связи и способов, описанных со ссылкой на способ 300 для аналогичных передач.

В блоке 428 процессор первого устройства для обработки данных может отправлять зашифрованную текстовую строку на третье устройство для обработки данных. Это передача может быть осуществ-

лена посредством или с использованием любого из каналов связи и способов, описанных со ссылкой на способ 300 для аналогичных передач.

В блоке 430 процессор третьего устройства для обработки данных может расшифровывать зашифрованную текстовую строку, принятую от первого устройства связи.

В блоке 432 процессор третьего устройства для обработки данных может повторно зашифровывать расшифрованную текстовую строку и может отправлять повторно зашифрованную текстовую строку на второе устройство для обработки данных. Это передача может быть осуществлена посредством или с использованием любого из каналов связи и способов, описанных со ссылкой на способ 300 для аналогичных передач. В различных воплощениях зашифрованная текстовая строка, принятая третьим устройством для обработки данных, может быть зашифрована в соответствии со способом или протоколом шифрования, согласованным или установленным между первым устройством для обработки данных и третьим устройством для обработки данных. Кроме того, третье устройство для обработки данных может повторно зашифровывать текстовую строку в соответствии со способом или протоколом шифрования, согласованным или установленным между вторым устройством для обработки данных и третьим устройством для обработки данных.

В блоке 434 процессор второго устройства для обработки данных может расшифровывать повторно зашифрованную текстовую строку, принятую от третьего устройства для обработки данных. В различных воплощениях процессор второго устройства для обработки данных может на этом этапе принимать нешифрованную текстовую строку непосредственно от первого устройства для обработки данных и повторно зашифрованную текстовую строку первого устройства для обработки данных от третьего устройства для обработки данных.

В блоке 436 процессор второго устройства может сравнивать текстовую строку от первого устройства для обработки данных и текстовую строку от третьего устройства для обработки данных.

В блоке 438 определения процессор второго устройства для обработки данных может определять, соответствуют ли текстовые строки друг другу.

В ответ на определение того, что текстовые строки не соответствуют друг другу (т.е. блок 438 определения="Нет"), процессор второго устройства для обработки данных может отправлять указание о том, что участие первого устройства для обработки данных в информационной транзакции не аутентифицировано, в блоке 440. Это передача может быть осуществлена посредством или с использованием любого из каналов связи и способов, описанных со ссылкой на способ 300 для аналогичных передач. В некоторых воплощениях операции блока 440 могут включать определение того, что участие первого устройства для обработки данных в информационной транзакции не аутентифицировано, в ответ на определение того, что текстовые строки не соответствуют друг другу, и отправку указания о том, что участие первого устройства для обработки данных в информационной транзакции не аутентифицировано. В некоторых воплощениях второе устройство для обработки данных может сохранять как часть журнала контроля указание о том, что участие первого устройства для обработки данных не аутентифицировано. В некоторых воплощениях третье устройство для обработки данных может сохранять как часть журнала контроля указание о том, что участие первого устройства для обработки данных не аутентифицировано.

В блоке 442 процессор второго устройства для обработки данных может предотвращать выполнение информационной транзакции. В некоторых воплощениях процессор второго устройства для обработки данных может предотвращать совершение одной или более операций информационной транзакции.

В ответ на определение того, что текстовые строки соответствуют друг другу (т.е. блок 438 определения="Да"), процессор второго устройства для обработки данных может отправлять указание о том, что участие первого устройства для обработки данных в информационной транзакции аутентифицировано, в блоке 444. Это передача может быть осуществлена посредством или с использованием любого из каналов связи и способов, описанных со ссылкой на способ 300 для аналогичных передач. В некоторых воплощениях операции блока 444 могут включать определение того, что участие первого устройства для обработки данных в информационной транзакции аутентифицировано, в ответ на определение того, что текстовые строки соответствуют друг другу, и отправку указания о том, что участие первого устройства для обработки данных в информационной транзакции аутентифицировано. В некоторых воплощениях второе устройство для обработки данных может сохранять как часть журнала контроля указание о том, что участие первого устройства для обработки данных аутентифицировано. В некоторых воплощениях третье устройство для обработки данных может сохранять как часть журнала контроля указание о том, что участие первого устройства для обработки данных аутентифицировано.

В блоке 446 процессор второго устройства для обработки данных может обеспечивать выполнение информационной транзакции. В некоторых воплощениях процессор второго устройства для обработки данных может совершать информационную транзакцию.

На фиг. 4B показана блок-схема способа 400a операций, выполняемых первым устройством для обработки данных как часть способа 400. Как показано на фиг. 1A-4D, способ 400a может быть реализован процессором (например, процессором 202 и/или подобным). В блоках 402, 406, 412, 424, 426 и 428 процессор первого устройства для обработки данных может выполнять операции аналогично пронумеро-

ванных блоков способа 400.

В опциональном блоке 445 процессор первого устройства для обработки данных может принимать подтверждение от второго устройства для обработки данных о соответствии идентифицирующей информации учетной записи первого устройства для обработки данных.

В блоке 447 процессор первого устройства для обработки данных может принимать от второго устройства для обработки данных запрос на предоставление временного идентификатора первого устройства для обработки данных.

В блоке 448 определения процессор первого устройства для обработки данных может определять, принимается или было принято указание о положительном результате подтверждения или указание об отрицательном результате подтверждения. В ответ на определение того, что указание об отрицательном результате подтверждения принимается или было принято (т.е. блок 448 определения="Отрицательный результат"), в блоке 450 процессор может прекращать выполнение операций способов 400 и 400a.

В ответ на определение того, что указание о положительном результате подтверждения принимается или было принято (т.е. блок 448 определения="Положительный результат"), процессор может выполнять операции блоков 424-428.

В блоке 452 определения процессор первого устройства для обработки данных может определять, принимается или было принято указание о том, что первое устройство для обработки данных аутентифицировано или не аутентифицировано. В ответ на определение того, что процессор принимает указание о том, что первое устройство для обработки данных не аутентифицировано (т.е. блок 452 определения="Не аутентифицировано"), процессор может прекращать выполнение операций способа 400 и 400a в блоке 454.

В ответ на определение того, что процессор принимает указание о том, что первое устройство для обработки данных аутентифицировано (т.е. блок 452 определения="Аутентифицировано"), процессор может выполнять информационную транзакцию в блоке 456.

На фиг. 4C показана блок-схема способа 400b операций, выполняемых вторым устройством для обработки данных как часть способа 400. Как показано на фиг. 1A-4D, способ 400a может быть реализован процессором (например, процессором 202 и/или подобным). В блоках 404, 408, 410, 414 и 436-442 процессор второго устройства для обработки данных может выполнять операции аналогично пронумерованных блоков способа 400.

В блоке 458 процессор второго устройства для обработки данных может принимать информацию, идентифицирующую учетную запись пользователя, от первого устройства для обработки данных.

В блоке 459 процессор второго устройства для обработки данных может принимать от первого устройства для обработки данных запрос на выполнение информационной транзакции.

В блоке 460 процессор второго устройства для обработки данных может принимать временный идентификатор от первого устройства для обработки данных (т.е. временный идентификатор первого устройства).

В блоке 462 определения процессор второго устройства для обработки данных может определять, принимается или было принято указание о положительном результате подтверждения первого устройства для обработки данных или об отрицательном результате подтверждения первого устройства для обработки данных.

В ответ на определение того, что указание об отрицательном результате подтверждения первого устройства для обработки данных, принимается или было принято (т.е. блок 462 определения="Отрицательный результат"), процессор может прекращать выполнение операций способа 400 и 400b в блоке 464.

В ответ на определение того, что указание о положительном результате подтверждения первого устройства для обработки данных принимается или было принято (т.е. блок 462 определения="Положительный результат"), процессор может продолжать выполнять информационную транзакцию.

В блоке 466 процессор может принимать нешифрованную текстовую строку от первого устройства для обработки данных.

В блоке 468 процессор может принимать повторно зашифрованную текстовую строку от третьего устройства для обработки данных.

В блоке 436 процессор второго устройства для обработки данных может сравнивать текстовую строку от первого устройства для обработки данных и текстовую строку от третьего устройства для обработки данных. В различных воплощениях процессор второго устройства для обработки данных может расшифровывать повторно зашифрованную текстовую строку, принятую от третьего устройства для обработки данных. В блоке 438 определения процессор второго устройства для обработки данных может определять, соответствуют ли текстовые строки друг другу (т.е. соответствует ли текстовая строка от первого устройства для обработки данных текстовой строке от третьего устройства для обработки данных).

В ответ на определение того, что текстовые строки не соответствуют друг другу (т.е. блок 438 определения="Нет"), процессор второго устройства для обработки данных может отправлять указание о

том, что участие первого устройства для обработки данных в информационной транзакции не аутентифицировано, в блоке 440.

В блоке 442 процессор второго устройства для обработки данных может предотвращать выполнение информационной транзакции. В некоторых воплощениях процессор второго устройства для обработки данных может предотвращать совершение одной или более операций информационной транзакции.

В ответ на определение того, что текстовые строки соответствуют друг другу (т.е. блок 438 определения="Да"), процессор второго устройства для обработки данных может отправлять указание о том, что участие первого устройства для обработки данных в информационной транзакции аутентифицировано, в блоке 444.

В блоке 446 второе устройство для обработки данных может обеспечивать выполнение информационной транзакции. В некоторых воплощениях второе устройство для обработки данных может совершать информационную транзакцию.

На фиг. 4D показана блок-схема способа 400c операций, выполняемых третьим устройством для обработки данных как часть способа 400. Как показано на фиг. 1A-4D, способ 400c может быть реализован процессором (например, процессором 202 и/или подобным). В блоках 416-422, 430, 432 процессор третьего устройства для обработки данных может выполнять операции аналогично пронумерованных блоков способа 400.

В блоке 470 процессор третьего устройства для обработки данных может принимать от первого устройства для обработки данных временный идентификатор первого устройства для обработки данных.

В блоке 472 процессор третьего устройства для обработки данных может принимать временный идентификатор первого устройства для обработки данных от второго устройства для обработки данных.

В блоке 416 процессор третьего устройства для обработки данных может сравнивать временный идентификатор первого устройства для обработки данных, принятый от первого устройства для обработки данных, и временный идентификатор первого устройства для обработки данных, принятый от второго устройства для обработки данных.

В блоке 474 процессор третьего устройства для обработки данных может принимать зашифрованную текстовую строку от первого устройства для обработки данных.

В блоке 476 определения процессор третьего устройства для обработки данных может определять, аутентифицировано или не аутентифицировано участие первого устройства для обработки данных в информационной транзакции.

В ответ на определение того, что участие первого устройства для обработки данных в информационной транзакции не аутентифицировано (т.е. блок 476 определения="Не аутентифицировано"), процессор третьего устройства для обработки данных может сохранять указание об отрицательном результате аутентификации в блоке 478.

В ответ на определение того, что участие первого устройства для обработки данных в информационной транзакции аутентифицировано (т.е. блок 476 определения="Аутентифицировано"), процессор третьего устройства для обработки данных может сохранять указание о положительном результате аутентификации в блоке 480.

На фиг. 5A показан способ 500 аутентификации первого устройства для обработки данных (например, устройства 102, 104, 184, 186 и 200 для обработки данных, показанного на фиг. 1B-2) со вторым устройством для обработки данных (например, устройством 106, 190-196 и 200 для обработки данных, показанным на фиг. 1B-2) и наоборот посредством взаимодействия с третьим устройством для обработки данных (например, 108, 188 и 200 на фиг. 1B-2) согласно некоторым воплощениям. Как показано на фиг. 1A-5B, способ 500 может быть реализован процессором (например, процессором 202 и/или подобным) устройства для обработки данных (т.е. процессором устройства). В блоках 302 и 304 процессор устройства может выполнять операции аналогично пронумерованных блоков способа 300.

В блоке 502 процессор системы обеспечения электронной безопасности (например, системы 114 обеспечения электронной безопасности) может осуществлять мониторинг системы связи. Например, система обеспечения электронной безопасности может выполнять мониторинг сети, запись вводимой с клавиатуры информации, обнаружение вторжения, анализ трафика или другую операцию для выполнения функций мониторинга сети или обеспечения безопасности.

В блоке 502 определения процессор системы обеспечения электронной безопасности может определять, обнаружен ли электронный злоумышленник или неавторизованный пользователь. В ответ на определение того, что электронный злоумышленник или неавторизованный пользователь не обнаружен (т.е. блок 504 определения="Нет"), процессор системы обеспечения электронной безопасности может продолжать выполнять мониторинг системы связи в блоке 502.

В ответ на определение того, что электронный злоумышленник или неавторизованный пользователь обнаружен (т.е. блок 504 определения="Да"), процессор системы обеспечения электронной безопасности может отправлять указание об электронном злоумышленнике или неавторизованном пользователе на третье устройство для обработки данных (например, третье устройство 108 для обработки данных) в блоке 506.

Процессор третьего устройства для обработки данных может принимать указание об электронном злоумышленнике или неавторизованном пользователе от системы обеспечения электронной безопасности. В ответ на указание об электронном злоумышленнике или неавторизованном пользователе от системы обеспечения электронной безопасности процессор третьего устройства для обработки данных может отправлять инструкцию на первое устройство для обработки данных (например, устройство 102 и 104 для обработки данных) и второе устройство для обработки данных (например, устройство 106 для обработки данных) на получение новых временных идентификаторов в блоке 330. Процессоры первого и второго устройств для обработки данных затем могут выполнять операции блоков 302 и 304.

В некоторых воплощениях третье устройство для обработки данных может отправлять инструкции на первое устройство для обработки данных и второе устройство для обработки данных в фоновом режиме, скрытом от конечного пользователя (например, когда первое устройство для обработки данных или второе устройство для обработки данных не предоставляет соответствующему пользователю указание о приеме инструкции от третьего устройства для обработки данных). В таких воплощениях на основании обнаружения электронного злоумышленника или неавторизованного пользователя третье устройство для обработки данных может отдавать инструкцию первому и второму устройствам для обработки данных, а также любым другим устройствам для обработки данных, задействованным в системе, на получение нового временного идентификатора и, таким образом, выполнять "глобальный перезапуск", который может не давать злоумышленнику или неавторизованному пользователю получать доступ к системе связи. В различных воплощениях скорость, с которой третье устройство для обработки данных может отправлять инструкцию на получение новых временных идентификаторов на различные устройства для обработки данных и с которой различные устройства для обработки данных могут получать соответствующий новый временный идентификатор, может быть ограничена только рабочей скоростью каждого устройства для обработки данных и задержкой связи в сети (например, запаздыванием связи). Количество времени, необходимое для отправки инструкций на первое и второе устройства для обработки данных и для получения первым и вторым устройствами для обработки данных новых временных идентификаторов, таким образом, меньше, чем, например, количество времени, необходимое для выдачи традиционным сертифицирующим органом новых сертификатов всем задействованным пользователям. Кроме того, способ 500 не требует осуществления операций вручную пользователем первого или второго устройства для обработки данных, таких как сброс пароля. Фактически, как описано выше, пользователь первого или второго устройства для обработки данных может продолжать использовать существующие учетные данные, такие как имя пользователя и пароль - даже после нарушения безопасности - поскольку существующие учетные данные могут использоваться для идентификации пользователя, но не используются в целях аутентификации.

В некоторых воплощениях система обеспечения электронной безопасности может быть сконфигурирована для приема команды или указания о том, что устройство для обработки данных должно быть деавторизовано от доступа к системе связи. Например, система обеспечения электронной безопасности может представлять собой компонент или элемент сетевой системы авторизации, или системы отдела кадров, или системы, которая предоставляет список авторизованных пользователей системы связи, или другой аналогичной системы. В таких воплощениях система обеспечения электронной безопасности может принимать команду или другое сообщение, указывающее, что авторизация устройства для обработки данных должна быть отменена или заблокирована. В некоторых воплощениях в ответ на прием указания о том, что был обнаружен неавторизованный пользователь или электронный злоумышленник, что должна быть отменена или заблокирована авторизация устройства для обработки данных, или другого аналогичного указания, третье устройство для обработки данных может отправлять инструкцию на первое устройство для обработки данных и/или второе устройство для обработки данных для получения нового временного идентификатора.

На фиг. 5B показана блок-схема способа 500a операций, выполняемых третьим устройством для обработки данных как часть способа 500. Как показано на фиг. 1A-5B, способ 500a может быть реализован процессором (например, процессором 202 и/или подобным).

В блоке 508 процессор третьего устройства для обработки данных может принимать от системы обеспечения электронной безопасности указание об электронном злоумышленнике или неавторизованном пользователе.

В блоке 510 процессор третьего устройства для обработки данных может отправлять инструкцию на первое устройство для обработки данных (например, устройство 102 и 104 для обработки данных) на получение нового временного идентификатора. Процессор первого устройства для обработки данных может переходить к блоку 302 способа 300 (фиг. 3A-3C).

В блоке 512 процессор третьего устройства для обработки данных может отправлять инструкцию на второе устройство для обработки данных (например, устройство 106 для обработки данных) на получение нового временного идентификатора. Процессор второго устройства для обработки данных может переходить к блоку 304 способа 300 (фиг. 3A, 3B и 3D).

На фиг. 6A показан способ 600 аутентификации первого устройства для обработки данных (например, устройства 102, 104, 184, 186 и 200 для обработки данных, показанного на фиг. 1B-2) относительно

второго устройства для обработки данных (например, устройства 106, 190-196 и 200 для обработки данных, показанного на фиг. 1B-2) и наоборот посредством взаимодействия с третьим устройством для обработки данных (например, 108, 188 и 200 на фиг. 1B-2) согласно некоторым воплощениям. На фиг. 6B показана блок-схема способа 600a операций, выполняемых процессором первого устройства для обработки данных как часть способа 600. На фиг. 6C показана блок-схема способа 600b операций, выполняемых процессором второго устройства для обработки данных как часть способа 600. На фиг. 6D показана блок-схема способа 600c операций, выполняемых процессором третьего устройства для обработки данных как часть способа 600.

В блоке 602 процессор первого устройства для обработки данных может отправлять небольшой фрагмент статической информации на третье устройство для обработки данных. Небольшой фрагмент статической информации может содержать воспринимаемый человеком индикатор, такой как, например, изображение, символ, звук, ритм или ритмический рисунок, инструкции гаптической обратной связи или другой аналогичный фрагмент информации, которая может быть представлена устройством для обработки данных.

В блоке 604 процессор третьего устройства для обработки данных может отправлять небольшой фрагмент статической информации на второе устройство для обработки данных. Третье устройство для обработки данных может отправлять небольшой фрагмент статической информации вместе с, параллельно с, до или после указания о положительном результате аутентификации первого устройства для обработки данных, которое третье устройство для обработки данных может отправлять на второе устройство для обработки данных в блоке 328.

В блоке 606 процессор второго устройства для обработки данных может отправлять небольшой фрагмент статической информации на первое устройство для обработки данных.

В блоке 608 процессор первого устройства для обработки данных может предоставлять небольшой фрагмент статической информации. В некоторых воплощениях предоставление небольшого фрагмента статической информации может включать предоставление воспринимаемого человеком указания, инструкции для которого включены в небольшой фрагмент статической информации. Воспринимаемое человеком указание может включать графическое изображение (такое как изображение, символ, эмодзи и т.п.), звук (такой как музыка, предупредительный шум, ритм или ритмический рисунок и т.п.), вибрацию (такую как устройство гаптической обратной связи) или другое воспринимаемое человеком указание. В некоторых воплощениях предоставление небольшого фрагмента статической информации может включать комбинацию двух или более из вышеперечисленного. В некоторых воплощениях небольшой фрагмент статической информации может быть выбран, создан или персонализирован пользователем первого устройства для обработки данных таким образом, чтобы небольшой фрагмент статической информации можно было легко распознать при предоставлении первым устройством для обработки данных.

Предоставление воспринимаемого человеком указания может обеспечивать легко воспринимаемое указание о том, что второе устройство для обработки данных приняло небольшой фрагмент статической информации от третьего устройства для обработки данных. Таким образом, предоставление воспринимаемого человеком указания первым устройством для обработки данных может обеспечивать дополнительное указание на первое устройство для обработки данных об идентификаторе второго устройства для обработки данных за счет проверки приема небольшого фрагмента статической информации вторым устройством для обработки данных от третьего устройства для обработки данных.

В некоторых воплощениях второе устройство для обработки данных может принимать небольшой фрагмент статической информации от третьего устройства для обработки данных и второе устройство для обработки данных может отправлять небольшой фрагмент статической информации непосредственно на первое устройство для обработки данных для указания о том, что второе устройство для обработки данных является аутентифицированным участником связи. Третье устройство для обработки данных после приема небольшого изображения от первого устройства для обработки данных и после аутентификации второго устройства для обработки данных может отправлять небольшое изображение на второе устройство для обработки данных. Второе устройство для обработки данных затем может отправлять изображение на первое устройство для обработки данных, например, для отображения первым устройством для обработки данных для обеспечения визуального указания об аутентификации второго устройства для обработки данных. В различных воплощениях использование такого небольшого фрагмента статической информации для обеспечения указания об аутентификации второго устройства для обработки данных может способствовать создавать препятствие, среди прочего, для атак типа целевой фишинг, атак "человек посередине" и других аналогичных атак на связь, предусматривающих перехват сообщения или исполнение роли устройства для обработки данных.

Например, при выполнении транзакции электронной торговли ("электронной коммерции") сервер электронной коммерции может принимать от третьего устройства для обработки данных (например, функционирующего как сервер аутентификации) небольшой файл изображения, принятый третьим устройством для обработки данных от первого устройства для обработки данных (например, пользовательского устройства). Сервер электронной коммерции затем может отправлять небольшой файл изображения на первое устройство для обработки данных для включения на сайт службы электронной коммерции

или для обеспечения некоторого другого визуального указания, отображаемого на первом устройстве для обработки данных при аутентификации второго устройства для обработки данных. Изображение, закодированное в небольшом файле изображения, может быть персонифицировано пользователем первого устройства для обработки данных и, таким образом, легко распознано им. Таким образом, в то время как в некоторых традиционных системах используется простое визуальное указание о том, что сетевая услуга защищена (например, символ "висячего замка" SSL), фактическую аутентификацию сетевой услуги может быть сложно или невозможно проверить. Кроме того, простое визуальное указание, как правило, является общим, при этом простое визуальное указание легко скопировать и использовать в мошеннических или злоумышленных услугах, таких как мошеннический сайт. Предоставление небольшого фрагмента статической информации в различных воплощениях представляет улучшение по сравнению с текущей системой обеспечения безопасности за счет обеспечения воспринимаемого и персонализированного указания о том, что второе устройство для обработки данных приняло небольшой фрагмент статической информации от третьего устройства для обработки данных. Это обеспечивает дополнительное указание пользователю первого устройства для обработки данных о том, что второе устройство для обработки данных аутентифицируется или было аутентифицировано третьим устройством для обработки данных.

На фиг. 6B показана блок-схема способа 600a операций, выполняемых первым устройством для обработки данных как часть способа 600. Как показано на фиг. 1A-6D, способ 600a может быть реализован процессором (например, процессором 202 и/или подобным). В блоках 302, 308, 314, 332-338, 340 и опциональном блоке 342 процессор первого устройства для обработки данных может выполнять операции аналогично пронумерованных блоков способов 300 и 300a.

В блоке 610 процессор первого устройства для обработки данных может отправлять небольшой фрагмент статической информации на третье устройство для обработки данных.

В блоке 612 процессор первого устройства для обработки данных может принимать небольшой фрагмент статической информации.

В блоке 614 процессор первого устройства для обработки данных может предоставлять небольшой фрагмент статической информации. Процессор первого устройства для обработки данных затем может выполнять операции блока 340 и опционального блока 342, как описано.

На фиг. 6C показана блок-схема способа 600b операций, выполняемых вторым устройством для обработки данных как часть способа 600. Как показано на фиг. 1A-6D, способ 600b может быть реализован процессором (например, процессором 202 и/или подобным). В блоках 304, 310, 316, 344-350, 352 и опциональном блоке 354 процессор второго устройства для обработки данных может выполнять операции аналогично пронумерованных блоков способов 300 и 300b.

В блоке 620 процессор второго устройства для обработки данных может принимать небольшой фрагмент статической информации от третьего устройства для обработки данных.

В блоке 622 процессор второго устройства для обработки данных может отправлять небольшой фрагмент статической информации на первое устройство для обработки данных. Процессор затем может выполнять операции блока 352 и опционального блока 354, как описано.

На фиг. 6D показана блок-схема способа 600c операций, выполняемых третьим устройством для обработки данных как часть способа 600. Как показано на фиг. 1A-6D, способ 600c может быть реализован процессором (например, процессором 202 и/или подобным). В блоках 306, 312, 318-330, 360 и 362 процессор третьего устройства для обработки данных может выполнять операции аналогично пронумерованных блоков способов 300 и 300d.

В блоке 630 процессор третьего устройства для обработки данных может принимать небольшой фрагмент статической информации от первого устройства для обработки данных.

В блоке 632 процессор третьего устройства для обработки данных может отправлять небольшой фрагмент статической информации от третьего устройства для обработки данных на второе устройство для обработки данных.

В различных воплощениях предлагается система, которая может аутентифицировать идентификатор устройства для обработки данных в системе связи на основании динамической информации каждого устройства для обработки данных, в отличие от текущей парадигмы общих секретов и статической информации. Различные воплощения улучшают работу каждого задействованного устройства для обработки данных за счет кардинального повышения уровня безопасности связи между задействованными устройствами для обработки данных. Кроме того, поскольку временный идентификатор каждого устройства для обработки данных периодически меняется, и каждое устройство для обработки данных периодически находится на связи с другими устройствами для обработки данных, отправляющими и/или принимающими новые временные идентификаторы, различные воплощения улучшают работу сети связи или системы электронной связи за счет повышения уровня безопасности связи. Различные воплощения также улучшают работу любой сети связи за счет надежной аутентификации идентификатора задействованного устройства для обработки данных, не опираясь на статическую идентификационную информацию, такую как общий секрет, которая может быть уязвимой к атаке в результате доступа и/или копирования.

Различные воплощения могут улучшать работу каждого задействованного устройства для обработ-

ки данных, а также всей системы связи, за счет обеспечения аутентификации задействованных устройств связи. Различные воплощения улучшают работу каждого задействованного устройства для обработки данных в широком диапазоне видов связи и/или контекстов информационных транзакций, включая ведение медицинских архивов, защищенную связь (например, для правительства, бизнеса, разведки и т.п.), системы ведения общественных архивов, системы голосования, системы финансового обслуживания, системы обеспечения безопасности брокерской деятельности и многие другие. Различные воплощения также могут улучшать работу Интернета вещей, а также связь между различными устройствами IoT или между устройствами IoT и контроллером устройств IoT, таким как маршрутизатор, сервер, концентратор IoT или другое аналогичное устройство. В частности, различные воплощения при реализации в среде IoT могут быть особенно полезны при предотвращении распределенных атак типа "отказ в обслуживании" (DDoS) без человеческого вмешательства. Различные воплощения могут улучшать работу системы связи за счет обеспечения выполнения неопровержимой информационной транзакции, в которой, поскольку участие конкретных устройств для обработки данных может быть аутентифицировано, процедура аутентификации может генерировать доказательство, ведущее к созданию предположения, что участник фактически был задействован в информационной транзакции.

Различные изображенные и описанные воплощения представлены исключительно в качестве примеров для иллюстрации различных признаков формулы изобретения. Однако признаки, показанные и описанные относительно любого указанного воплощения, не обязательно ограничены связанным воплощением и могут быть использованы или скомбинированы с другими воплощениями, которые показаны и описаны. Кроме того, формула изобретения не должна рассматриваться, как ограниченная любым из приведенных в качестве примера воплощений. Например, одна или более из операций способов 300, 300a, 300b, 300c, 400, 400a, 400b, 400c, 500, 500a, 600, 600a, 600b и 600c может быть заменена или скомбинирована с одной или более операциями способов 300, 300a, 300b, 300c, 400, 400a, 400b, 400c, 500, 500a, 600, 600a, 600b и 600c.

На фиг. 7 показана блок-схема компонентов мобильного устройства 700 беспроводной связи, подходящего для реализации различных воплощений. Как показано на фиг. 1A-7, мобильное устройство 700 беспроводной связи может содержать процессор 702, соединенный с контроллером 706 сенсорного экрана и внутренним запоминающим устройством 704. Процессор 702 может представлять собой одну или более многоядерных интегральных схем, предназначенных для выполнения общих или специальных задач по обработке данных. Внутреннее запоминающее устройство 704 может представлять собой энергозависимое или энергонезависимое запоминающее устройство, а также может представлять собой защищенное и/или зашифрованное запоминающее устройство, или незащищенное и/или нешифрованное запоминающее устройство или любую их комбинацию. Контроллер 706 сенсорного экрана и процессор 702 также могут быть соединены с сенсорным экраном 712, таким как резистивный сенсорный экран, емкостный сенсорный экран, инфракрасный сенсорный экран и т.п. Дополнительно дисплей мобильного устройства 700 беспроводной связи не обязательно должен иметь сенсорную функцию.

Мобильное устройство 700 беспроводной связи может содержать два или более приемопередатчиков 708 радиосигналов (например, Peanut, Bluetooth, Zigbee, Wi-Fi, радиочастотный (RF) прибор и т.п.) и антенн 710 для отправки и приема сообщений, которые соединены друг с другом и/или с процессором 702. Приемопередатчики 708 и антенны 710 могут использоваться с вышеуказанной схемой для реализации различных стеков протоколов и интерфейсов беспроводной передачи. Мобильное устройство 700 беспроводной связи может содержать один или более чипов 716 беспроводного модема сотовой сети, соединенных с процессором и антеннами 710, что обеспечивает связь при помощи двух или более сотовых сетей посредством двух или более технологий радиодоступа.

Мобильное устройство 700 беспроводной связи может содержать интерфейс 718 подключения периферийных беспроводных устройств, соединенный с процессором 702. Интерфейс 718 подключения периферийных беспроводных устройств может быть сконфигурирован исключительно для приема одного типа подключения или может быть сконфигурирован для приема различных типов физических и коммуникационных подключений, общераспространенных или специализированных, таких как USB, FireWire, Thunderbolt или PCIe. Интерфейс 718 подключения периферийных беспроводных устройств также может быть соединен с аналогично сконфигурированным портом подключения периферийных беспроводных устройств (не показан).

Мобильное устройство 700 беспроводной связи также может содержать динамики 714 для обеспечения аудиовыходов. Мобильное устройство 700 беспроводной связи также может содержать корпус 720, выполненный из пластмассы, металла или комбинации материалов и предназначенный для вмещения всех или некоторых из компонентов, описанных в настоящем документе. Мобильное устройство 700 беспроводной связи может содержать источник 722 питания, соединенный с процессором 702, такой как одноразовая или перезаряжаемая батарея. Перезаряжаемая батарея также может быть соединена с портом подключения периферийных беспроводных устройств для получения зарядного тока от источника, внешнего по отношению к мобильному устройству 700 беспроводной связи. Мобильное устройство 700 беспроводной связи также может содержать физическую кнопку 724 для приема пользовательского ввода. Мобильное устройство 700 беспроводной связи также может содержать кнопку 726 питания для

включения и выключения мобильного устройства 700 беспроводной связи.

Другие формы устройств для обработки данных также могут быть предпочтительными исходя из различных аспектов. Такие устройства для обработки данных, как правило, включают компоненты, изображенные на фиг. 8, на которой показан приведенный в качестве примера портативный компьютер 800. Как показано на фиг. 1A-8, компьютер 800 в целом содержит процессор 801, соединенный с энергозависимым запоминающим устройством 802 и энергонезависимым запоминающим устройством большой емкости, таким как дисковый накопитель 803. Компьютер 800 также может содержать дисковод 804 для компакт-дисков (CD) и/или DVD, соединенный с процессором 801. Компьютер 800 также может содержать ряд портов подключения, соединенных с процессором 801 для установления информационных соединений или размещения внешних запоминающих устройств, таких как схема 805 сетевого подключения для подключения процессора 801 к сети. Компьютер 800 также может содержать дисплей 807, клавиатуру 808, указывающее устройство, такое как трекпад 810, и другие аналогичные устройства.

В различных воплощениях может использоваться устройство для обработки данных как сетевой элемент сети связи. Такие сетевые элементы, как правило, могут содержать, по меньшей мере, компоненты, изображенные на фиг. 9, на которой показан приведенный в качестве примера сетевой элемент, серверное устройство 900. Как показано на фиг. 1A-9, серверное устройство 900, как правило, может содержать процессор 901, соединенный с энергозависимым запоминающим устройством 902 и энергонезависимым запоминающим устройством большой емкости, таким как дисковый накопитель 903. Серверное устройство 900 также может содержать устройство для доступа к периферийному запоминающему устройству, такое как дисковод для гибких дисков или дисковод 906 для компакт-дисков (CD) или цифровых видеодисков (DVD), соединенный с процессором 901. Серверное устройство 900 также может содержать порты 904 (или интерфейсы) доступа к сети, соединенные с процессором 901 для установления информационных соединений с сетью, такой как Интернет и/или локальная вычислительная сеть, соединенная с другими компьютерами и серверами системы. Аналогично, серверное устройство 900 может содержать дополнительные порты доступа, такие как USB, Firewire, Thunderbolt и т.п. для подключения к периферийным устройствам, внешнему запоминающему устройству или другим устройствам.

Процессоры 702, 801, 901 могут представлять собой любой программируемый микропроцессор, микрокомпьютер или чип или чипы с множеством процессоров, которые могут быть сконфигурированы программными инструкциями (приложениями) для выполнения различных функций, включая функции различных аспектов, описанных ниже. В некоторых мобильных устройствах может быть предусмотрено множество процессоров 702, например один процессор, выделенный для функций беспроводной связи, и один процессор, выделенные для запуска других приложений. Как правило, программные приложения могут храниться во внутреннем запоминающем устройстве 704, 802, 902 до получения к ним доступа и их загрузки в процессор 702, 801, 901. Процессор 702, 801, 901 может содержать внутреннее запоминающее устройство, достаточное для хранения программных инструкций приложения.

Различные воплощения могут быть реализованы в любом количестве одно- и многопроцессорных систем. В целом, процессы исполняются в процессоре за короткие интервалы времени, поэтому кажется, что множество процессов выполняются одновременно на одном процессоре. Когда процесс удаляется из процессора в конце интервала времени, информация, относящаяся к текущему рабочему состоянию процесса, сохраняется в запоминающем устройстве, поэтому процесс может беспроблемно возобновить свою работу при возвращении к исполнению на процессоре. Эти данные о рабочем состоянии могут включать адресное пространство процесса, стековое пространство, виртуальное адресное пространство, изображение набора регистров (например, программный счетчик, указатель стека, регистр инструкций, слово состояния программы и т.п.), учетную информацию, разрешения, ограничения доступа и информацию о состоянии.

Процесс может создавать другие процессы, и созданный процесс (т.е. порожденный процесс) может наследовать некоторые из разрешений и ограничений доступа (т.е. контекст) создающего процесса (т.е. порождающего процесса). Процесс может представлять собой тяжеловесный процесс, который содержит множество легковесных процессов или потоков, которые представляют собой процессы, совместно использующие все или части их контекста (например, адресное пространство, стек, разрешения и/или ограничения доступа и т.п.) с другими процессами/потоками. Таким образом, один процесс может содержать множество легковесных процессов или потоков, которые совместно используют, имеют доступ к и/или функционируют в одном контексте (т.е. контексте процессора).

Вышеизложенные описания блок-схем способа и процесса представлены исключительно в качестве иллюстративных примеров и не требуют или не подразумевают, что блоки различных воплощений должны выполняться в представленном порядке. Как будет понятно специалисту в области техники, блоки в вышеизложенных воплощениях могут выполняться в любом порядке. Слова, такие как "после этого", "затем", "потом" и т.п. не предназначены для ограничения порядка выполнения блоков; эти слова просто используются для проведения читателя через описание способов. Кроме того, любая ссылка на элемент в единственном числе не должна рассматриваться, как ограничивающая элемент только единственным числом.

Различные иллюстративные логические блоки, модули, схемы и блоки алгоритмов, описанные при-

менительно к воплощениям, раскрытым в настоящем описании, могут быть реализованы в виде электронных аппаратных средств, компьютерного программного обеспечения или их сочетаний. Для того чтобы более ясно показать эту взаимозаменимость аппаратных средств и программного обеспечения, различные иллюстративные компоненты, блоки, модули, схемы и блоки были описаны выше в сущности в отношении их функциональности. Реализация такой функциональности в виде аппаратных средств или программного обеспечения зависит от конкретного применения и ограничений в плане конструкции применительно ко всей системе. Опытные специалисты могут реализовать описанную функциональность различными способами для каждого конкретного применения, но такие решения в плане реализации не должны интерпретироваться как выходящие за рамки объема формулы изобретения.

Аппаратные средства, используемые для реализации различных иллюстративных логических моделей, логических блоков, модулей и схем, описанных применительно к воплощениям, раскрытым в настоящем описании, могут быть реализованы или выполнены с помощью универсального процессора, процессора цифровой обработки сигналов (DSP), специализированной интегральной схемы (ASIC), программируемой пользователем вентильной матрицы (FPGA) или другого программируемого логического устройства, логического элемента на дискретных компонентах или транзисторных логических схем, отдельных компонентов аппаратных средств или любого их сочетания, предназначенного для выполнения функций, раскрытых в настоящем описании. Универсальный процессор может представлять собой микропроцессор, однако, альтернативно, указанный процессор может представлять собой любой стандартный процессор, контроллер, микроконтроллер или конечную машину. Процессор также может быть реализован в виде сочетания устройств связи, например сочетания DSP и микропроцессора, множества микропроцессоров, одного или более микропроцессоров в сочетании с DSP ядром или в виде любой другой подобной конфигурации. Альтернативно, некоторые блоки или способы могут выполняться схемами, характерными для соответствующих функций.

В различных воплощениях описанные функции могут быть реализованы в аппаратных средствах, программном обеспечении, прошивке или любом их сочетании. При реализации в программном обеспечении функции могут храниться в виде одной или более инструкций или кода на постоянном машиночитаемом носителе или постоянном читаемом процессором носителе. Операции способа или алгоритма, раскрытые в настоящем описании, могут быть воплощены в выполняемом процессором программном модуле, который может находиться на постоянном машиночитаемом или читаемом процессором информационном носителе. Постоянный машиночитаемый или читаемый процессором информационный носитель может представлять собой любой информационный носитель, к которому может получать доступ компьютер или процессор. В качестве неограничивающих примеров такой постоянный машиночитаемый или читаемый процессором носитель может включать RAM, ROM, EEPROM, флеш-память, CD-ROM или другое оптическое запоминающее устройство, магнитное дисковое запоминающее устройство или другие магнитные запоминающие устройства, или любой другой носитель, который может быть использован для хранения необходимого программного кода в виде инструкций или структур данных, и к которому компьютер может получать доступ. Термин "магнитный диск" и "оптический диск", используемые в настоящем описании, включают компакт-диск (CD), лазерный диск, цифровой универсальный диск (DVD), флоппи-диск, блюрей диск, при этом данные с флоппи-диска обычно воспроизводятся магнитным способом, а с компакт-диска, лазерного диска, оптического диска, DVD-диска и блюрей диска - оптическим способом посредством лазеров. Предполагается, что сочетания вышеприведенных технологий также входят в объем охраны, обеспечиваемый терминами "постоянный машиночитаемый и читаемый процессором носитель". Кроме того, операции способа или алгоритма могут представлять собой один или любую комбинацию, или набор кодов и/или инструкций на постоянном читаемом компьютером носителе и/или машинно-читаемом носителе, который может быть включен в компьютерный программный продукт.

Вышеприведенное описание раскрытых воплощений обеспечено для того, чтобы любой специалист в данной области техники мог изготовить или использовать объект формулы изобретения. Различные модификации этих воплощений будут очевидны для специалистов в данной области техники, и общие принципы, раскрытые в настоящем документе, могут быть использованы применительно к другим воплощениям без отклонения от объема формулы изобретения. Таким образом, настоящее изобретение не следует рассматривать как ограниченное воплощениями, раскрытыми в настоящем описании, его следует рассматривать как обеспечивающее наиболее широкий объем охраны, соответствующий приведенной ниже формуле изобретения, а также принципам и новым признакам, раскрытым в настоящем описании.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система для аутентификации первого устройства для обработки данных относительно второго устройства для обработки данных посредством взаимодействия с третьим устройством для обработки данных, содержащая

первое устройство для обработки данных, содержащее

первый интерфейс связи; и

первый процессор, соединенный с упомянутым первым интерфейсом связи и сконфигурированный с выполняемыми процессором инструкциями для выполнения операций, содержащих

получение эфемерного первого временного идентификатора на первом устройстве для обработки данных;

отправку первого временного идентификатора на второе устройство для обработки данных и на третье устройство для обработки данных;

прием эфемерного второго временного идентификатора от второго устройства для обработки данных;

отправку первого запроса на аутентификацию, содержащего второй временный идентификатор, на третье устройство для обработки данных; и

прием от третьего устройства для обработки данных указания о том, аутентифицировано ли второе устройство для обработки данных;

второе устройство для обработки данных, содержащее

второй интерфейс связи; и

второй процессор, соединенный с упомянутым вторым интерфейсом связи и сконфигурированный с выполняемыми процессором инструкциями для выполнения операций, содержащих

получение упомянутого второго временного идентификатора на упомянутом втором устройстве для обработки данных;

отправку упомянутого второго временного идентификатора на первое устройство для обработки данных и на третье устройство для обработки данных;

прием упомянутого первого временного идентификатора от упомянутого первого устройства для обработки данных;

отправку второго запроса на аутентификацию, содержащего упомянутый первый временный идентификатор, на упомянутое третье устройство для обработки данных; и

прием от третьего устройства для обработки данных указания о том, аутентифицировано ли первое устройство для обработки данных;

и третье устройство для обработки данных, содержащее

третий интерфейс связи; и

третий процессор, соединенный с упомянутым третьим интерфейсом связи и сконфигурированный с выполняемыми процессором инструкциями для выполнения операций, содержащих

прием упомянутого первого временного идентификатора от первого устройства для обработки данных;

прием упомянутого второго запроса на аутентификацию;

определение того, соответствует ли первый временный идентификатор от первого устройства для обработки данных первому временному идентификатору от второго устройства для обработки данных;

отправку на второе устройство для обработки данных указания о том, аутентифицировано ли первое устройство для обработки данных, на основании определения того, соответствует ли первый временный идентификатор от первого устройства для обработки данных первому временному идентификатору от второго устройства для обработки данных;

прием второго временного идентификатора от второго устройства для обработки данных;

прием упомянутого первого запроса на аутентификацию;

определение того, соответствует ли второй временный идентификатор от первого устройства для обработки данных второму временному идентификатору от второго устройства для обработки данных; и

отправку на первое устройство для обработки данных указания о том, аутентифицировано ли второе устройство для обработки данных, на основании определения того, соответствует ли второй временный идентификатор от первого устройства для обработки данных второму временному идентификатору от второго устройства для обработки данных.

2. Система по п.1, в которой процессор третьего устройства для обработки данных выполнен с возможностью исполнения операций, дополнительно содержащих

отправку инструкции на каждое из первого устройства для обработки данных и второго устройства для обработки данных на получение эфемерного нового временного идентификатора.

3. Система по п.2, в которой процессор третьего устройства для обработки данных выполнен с возможностью исполнения операций, при этом отправка инструкции на каждое из первого устройства для обработки данных и второго устройства для обработки данных на получение упомянутого нового временного идентификатора содержит

отправку инструкции на каждое из первого устройства для обработки данных и второго устройства для обработки данных на получение упомянутого нового временного идентификатора в ответ на определение того, что упомянутый первый временный идентификатор от второго устройства для обработки данных не соответствует упомянутому первому временному идентификатору от первого устройства для обработки данных.

4. Система по п.2, в которой процессор третьего устройства для обработки данных выполнен с возможностью исполнения операций, при этом отправка инструкции на каждое из первого устройства для

обработки данных и второго устройства для обработки данных на получение упомянутого нового временного идентификатора содержит

отправку инструкции на каждое из первого устройства для обработки данных и второго устройства для обработки данных на получение нового временного идентификатора в ответ на определение того, что упомянутый второй временный идентификатор от первого устройства для обработки данных не соответствует упомянутому второму временному идентификатору от второго устройства для обработки данных.

5. Система по п.1, в которой каждый из процессора первого устройства для обработки данных, процессора второго устройства для обработки данных и процессора третьего устройства для обработки данных выполнен с возможностью повторения соответствующих им операций с частотой, которая меньше, чем определенный интервал времени, необходимый злоумышленнику для получения и использования упомянутых первого и второго временных идентификаторов.

6. Система по п.1, в которой каждый из процессора первого устройства для обработки данных, процессора второго устройства для обработки данных и процессора третьего устройства для обработки данных выполнен с возможностью повторения соответствующих им операций с частотой, которая меньше, чем определенное время, необходимое злоумышленнику для получения и использования первого, второго и третьего временных идентификаторов.

7. Система по п.1, в которой процессор первого устройства для обработки данных выполнен с возможностью исполнения операций, дополнительно содержащих

генерирование текстовой строки и генерирование зашифрованной версии текстовой строки;

отправку сгенерированной текстовой строки на второе устройство для обработки данных;

отправку сгенерированной зашифрованной текстовой строки на третье устройство для обработки данных; и

прием от второго устройства для обработки данных указания о том, аутентифицировано ли первое устройство для обработки данных, на основании текстовой строки, отправленной на второе устройство для обработки данных, и зашифрованной текстовой строки, отправленной на третье устройство для обработки данных.

8. Система по п.7, в которой процессор первого устройства для обработки данных выполнен с возможностью исполнения операций, дополнительно содержащих

выполнение информационной транзакции со вторым устройством для обработки данных в ответ на прием от второго устройства для обработки данных указания о том, что первое устройство для обработки данных аутентифицировано.

9. Система по п.7, в которой процессор третьего устройства для обработки данных выполнен с возможностью исполнения операций, дополнительно содержащих

расшифровку зашифрованной текстовой строки от первого устройства для обработки данных; и

повторную зашифровку расшифрованной текстовой строки и отправку повторно зашифрованной текстовой строки на второе устройство для обработки данных для обеспечения сравнения вторым устройством для обработки данных повторно зашифрованной текстовой строки и текстовой строки, отправленной от первого устройства для обработки данных на второе устройство для обработки данных.

10. Система по п.7, в которой процессор второго устройства для обработки данных выполнен с возможностью исполнения операций, дополнительно содержащих

прием текстовой строки от первого устройства для обработки данных;

прием повторно зашифрованной текстовой строки от третьего устройства для обработки данных;

определение того, соответствуют ли друг другу текстовая строка от первого устройства для обработки данных и повторно зашифрованная текстовая строка от третьего устройства для обработки данных; и

отправку на одно или более из первого устройства для обработки данных и третьего устройства для обработки данных указания о том, аутентифицировано ли участие первого устройства для обработки данных, в ответ на определение того, соответствуют ли друг другу текстовая строка от первого устройства для обработки данных и повторно зашифрованная текстовая строка от третьего устройства для обработки данных.

11. Система по п.10, в которой процессор третьего устройства для обработки данных выполнен с возможностью исполнения операций, дополнительно содержащих

прием указания о том, аутентифицировано ли участие первого устройства для обработки данных; и

сохранение указания о том, аутентифицировано ли участие первого устройства для обработки данных.

12. Система по п.1, в которой процессор первого устройства для обработки данных выполнен с возможностью исполнения операций, дополнительно содержащих

отправку фрагмента статической информации на третье устройство для обработки данных;

прием от второго устройства для обработки данных упомянутого фрагмента статической информации на основании определения того, что первый временный идентификатор от второго устройства для обработки данных соответствует первому временному идентификатору от первого устройства для обра-

ботки данных; и

представление упомянутого фрагмента статической информации на первом устройстве для обработки данных.

13. Система по п.12, в которой процессор первого устройства для обработки данных выполнен с возможностью исполнения операций, при этом упомянутый фрагмент статической информации содержит воспринимаемый человеком индикатор.

14. Система по п.1, в которой процессор второго устройства для обработки данных выполнен с возможностью исполнения операций, дополнительно содержащих

прием от третьего устройства для обработки данных фрагмента статической информации от первого устройства для обработки данных; и

отправку на первое устройство для обработки данных упомянутого фрагмента статической информации на основании определения того, что первый временный идентификатор от второго устройства для обработки данных соответствует первому временному идентификатору от первого устройства для обработки данных.

15. Система по п.1, в которой процессор третьего устройства для обработки данных выполнен с возможностью исполнения операций, дополнительно включающих

прием фрагмента статической информации от первого устройства для обработки данных; и

отправку на второе устройство для обработки данных упомянутого фрагмента статической информации на основании определения того, что первый временный идентификатор от второго устройства для обработки данных соответствует первому временному идентификатору от первого устройства для обработки данных.

16. Система по п.1, в которой первое устройство для обработки данных содержит устройство Интернета вещей (IoT).

17. Первое устройство для обработки данных, содержащее

интерфейс связи; и

процессор, соединенный с упомянутым интерфейсом связи и сконфигурированный с выполняемыми процессором инструкциями для выполнения операций, содержащих

получение эфемерного первого временного идентификатора;

отправку упомянутого первого временного идентификатора на второе устройство для обработки данных и на третье устройство для обработки данных;

прием эфемерного второго временного идентификатора от второго устройства для обработки данных;

отправку запроса на аутентификацию, содержащего упомянутый второй временный идентификатор, на третье устройство для обработки данных;

определение того, принято ли указание о положительном результате аутентификации или указание об отрицательном результате аутентификации от третьего устройства для обработки данных; и

выполнение информационной транзакции со вторым устройством для обработки данных в ответ на определение того, что принято указание о положительном результате аутентификации,

при этом процессор дополнительно сконфигурирован с выполняемыми процессором инструкциями для повторения операций с частотой, которая меньше, чем определенный интервал времени, необходимый злоумышленнику для получения и использования первого и второго временных идентификаторов.

18. Первое устройство для обработки данных по п.17, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

прием инструкции от третьего устройства для обработки данных на получение нового временного идентификатора и

получение эфемерного нового первого временного идентификатора на основании инструкции.

19. Первое устройство для обработки данных по п.17, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

определение того, что срок действия первого временного идентификатора истек; и

получение эфемерного нового первого временного идентификатора на основании определения того, что срок действия первого временного идентификатора истек.

20. Первое устройство для обработки данных по п.17, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

выполнение действия по обеспечению безопасности в ответ на определение того, что принято указание об отрицательном результате аутентификации.

21. Первое устройство для обработки данных по п.17, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

отправку на второе устройство для обработки данных запроса на выполнение информационной транзакции;

прием от второго устройства для обработки данных указания о том, аутентифицировано ли первое устройство для обработки данных; и

выполнение информационной транзакции в ответ на прием указания о том, что первое устройство

для обработки данных аутентифицировано.

22. Первое устройство для обработки данных по п.21, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

прием запроса от второго устройства для обработки данных на предоставление первого временного идентификатора на основании запроса на выполнение информационной транзакции,

при этом отправка первого временного идентификатора на второе устройство для обработки данных и на третье устройство для обработки данных основана на запросе от второго устройства для обработки данных на предоставление первого временного идентификатора.

23. Первое устройство для обработки данных по п.21, в котором процессор первого устройства для обработки данных выполнен с возможностью исполнения операций, дополнительно содержащих

генерирование текстовой строки и генерирование зашифрованной версии текстовой строки;

отправку сгенерированной текстовой строки на второе устройство для обработки данных;

отправку сгенерированной зашифрованной текстовой строки на третье устройство для обработки данных; и

прием от второго устройства для обработки данных указания о том, аутентифицировано ли первое устройство для обработки данных, на основании текстовой строки, отправленной на второе устройство для обработки данных, и зашифрованной текстовой строки, отправленной на третье устройство для обработки данных.

24. Первое устройство для обработки данных по п.17, в котором первое устройство для обработки данных содержит устройство Интернета вещей (IoT).

25. Устройство для обработки данных, содержащее

интерфейс связи; и

процессор, соединенный с интерфейсом связи и сконфигурированный с выполняемыми процессором инструкциями для выполнения операций, содержащих

прием от первого другого устройства для обработки данных запроса на выполнение информационной транзакции;

прием от упомянутого первого другого устройства для обработки данных эфемерного временного идентификатора упомянутого первого другого устройства для обработки данных;

отправку запроса, содержащего упомянутый временный идентификатор, на второе другое устройство для обработки данных для подтверждения идентификатора первого другого устройства для обработки данных;

прием от упомянутого второго другого устройства для обработки данных указания о том, подтвержден ли идентификатор упомянутого первого другого устройства для обработки данных; и

отправку подтверждения и указания на выполнение информационной транзакции на основании данных о верификации идентификатора упомянутого первого другого устройства для обработки данных,

при этом процессор дополнительно сконфигурирован с выполняемыми процессором инструкциями для повторения операций с частотой, которая меньше, чем определенный интервал времени, необходимый злоумышленнику для получения и использования временного идентификатора.

26. Устройство для обработки данных по п.25, в котором упомянутый процессор выполнен с возможностью исполнения операций, дополнительно содержащих

отправку запроса на упомянутое первое другое устройство для обработки данных на предоставление временного идентификатора первого другого устройства для обработки данных на основании запроса на выполнение информационной транзакции.

27. Устройство для обработки данных по п.25, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

прием текстовой строки от упомянутого первого другого устройства для обработки данных;

прием повторно зашифрованной текстовой строки от упомянутого второго другого устройства для обработки данных;

определение того, соответствуют ли друг другу текстовая строка от упомянутого первого другого устройства для обработки данных и повторно зашифрованная текстовая строка от упомянутого второго другого устройства для обработки данных; и

отправку на одно или более из упомянутых первого другого устройства для обработки данных и второго другого устройства для обработки данных указания о том, аутентифицировано ли участие первого другого устройства для обработки данных в ответ на определение того, соответствуют ли друг другу текстовая строка от упомянутого первого другого устройства для обработки данных и повторно зашифрованная текстовая строка от упомянутого второго другого устройства для обработки данных.

28. Устройство для обработки данных по п.27, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

выполнение информационной транзакции на основании определения того, что текстовая строка от упомянутого первого другого устройства для обработки данных и повторно зашифрованная текстовая строка от упомянутого второго другого устройства для обработки данных соответствуют друг другу.

29. Устройство для обработки данных, выполненное с возможностью связи с первым другим уст-

ройством для обработки данных и вторым другим устройством для обработки данных, содержащее

интерфейс связи; и

процессор, соединенный с интерфейсом связи и сконфигурированный с выполняемым процессором инструкциями для выполнения операций, содержащих

прием эфемерного первого временного идентификатора от первого другого устройства для обработки данных;

прием запроса на аутентификацию, содержащего упомянутый первый временный идентификатор, от второго другого устройства для обработки данных;

определение того, соответствует ли упомянутый первый временный идентификатор от первого другого устройства для обработки данных первому временному идентификатору от второго другого устройства для обработки данных; и

отправку на второе другое устройство для обработки данных указания о том, аутентифицировано ли первое другое устройство для обработки данных, на основании определения того, соответствует ли упомянутый первый временный идентификатор от первого другого устройства для обработки данных упомянутому первому временному идентификатору от второго другого устройства для обработки данных,

при этом процессор дополнительно сконфигурирован с выполняемыми процессором инструкциями для повторения операций с частотой, которая меньше, чем определенный интервал времени, необходимый злоумышленнику для получения и использования первого временного идентификатора.

30. Устройство для обработки данных по п.29, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

прием эфемерного второго временного идентификатора от второго другого устройства для обработки данных;

прием запроса на аутентификацию, содержащего упомянутый второй временный идентификатор, от первого другого устройства для обработки данных;

определение того, соответствует ли упомянутый второй временный идентификатор от второго другого устройства для обработки данных упомянутому второму временному идентификатору от первого другого устройства для обработки данных; и

отправку на упомянутое первое другое устройство для обработки данных указания о том, аутентифицировано ли второе другое устройство для обработки данных, на основании определения того, соответствует ли упомянутый второй временный идентификатор от второго другого устройства для обработки данных упомянутому второму временному идентификатору от первого другого устройства для обработки данных.

31. Устройство для обработки данных по п.30, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

отправку на упомянутое первое другое устройство для обработки данных указания о положительном результате аутентификации упомянутого второго другого устройства для обработки данных в ответ на определение того, что упомянутый второй временный идентификатор от второго другого устройства для обработки данных соответствует упомянутому второму временному идентификатору от упомянутого первого другого устройства для обработки данных.

32. Устройство для обработки данных по п.30, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

отправку на первое другое устройство для обработки данных указания об отрицательном результате аутентификации второго другого устройства для обработки данных в ответ на определение того, что упомянутый второй временный идентификатор от второго другого устройства для обработки данных не соответствует упомянутому второму временному идентификатору от первого другого устройства для обработки данных.

33. Устройство для обработки данных по п.29, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

отправку на упомянутое второе другое устройство для обработки данных указания о положительном результате аутентификации первого другого устройства для обработки данных в ответ на определение того, что упомянутый первый временный идентификатор от первого другого устройства для обработки данных соответствует упомянутому первому временному идентификатору от второго другого устройства для обработки данных.

34. Устройство для обработки данных по п.29, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

отправку на второе другое устройство для обработки данных указания об отрицательном результате аутентификации первого другого устройства для обработки данных в ответ на определение того, что упомянутый первый временный идентификатор от первого другого устройства для обработки данных не соответствует упомянутому первому временному идентификатору от второго другого устройства для обработки данных.

35. Устройство для обработки данных по п.29, в котором процессор выполнен с возможностью ис-

полнения операций, дополнительно содержащих

определение того, что срок действия первого временного идентификатора истек; и

отправку инструкции на первое другое устройство для обработки данных на получение нового временного идентификатора в ответ на определение того, что срок действия первого временного идентификатора истек.

36. Устройство для обработки данных по п.29, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

определение того, что срок действия второго временного идентификатора истек; и

отправку инструкции на второе другое устройство для обработки данных на получение нового временного идентификатора в ответ на определение того, что срок действия второго временного идентификатора истек.

37. Устройство для обработки данных по п.29, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

прием от системы обеспечения электронной безопасности указания о неавторизованном пользователе; и

отправку инструкции на одно или более из первого другого устройства для обработки данных и второго устройства для обработки данных на получение эфемерного нового временного идентификатора в ответ на указание о неавторизованном пользователе.

38. Устройство для обработки данных по п.29, в котором процессор выполнен с возможностью исполнения операций, дополнительно содержащих

прием от упомянутого первого другого устройства для обработки данных зашифрованной текстовой строки и расшифровку зашифрованной текстовой строки;

повторную зашифровку расшифрованной текстовой строки и отправку повторно зашифрованной текстовой строки на упомянутое второе другое устройство для обработки данных;

прием указания от упомянутого второго другого устройства для обработки данных о том, аутентифицировано ли участие упомянутого первого другого устройства для обработки данных; и

сохранение указания о том, аутентифицировано ли участие упомянутого первого другого устройства для обработки данных.

39. Способ аутентификации взаимодействий между первым устройством для обработки данных и вторым устройством для обработки данных с помощью третьего устройства для обработки данных, причем способ содержит

получение эфемерного первого временного идентификатора на первом устройстве для обработки данных;

отправку упомянутого первого временного идентификатора на второе устройство для обработки данных и на третье устройство для обработки данных;

прием на втором устройстве для обработки данных упомянутого первого временного идентификатора от первого устройства для обработки данных;

получение эфемерного второго временного идентификатора на втором устройстве для обработки данных;

отправку упомянутого второго временного идентификатора от второго устройства для обработки данных на первое устройство для обработки данных и на третье устройство для обработки данных;

прием на первом устройстве для обработки данных упомянутого второго временного идентификатора от второго устройства для обработки данных;

отправку первого запроса на аутентификацию, содержащего упомянутый второй временный идентификатор, от первого устройства для обработки данных на третье устройство для обработки данных;

отправку второго запроса на аутентификацию, содержащего первый временный идентификатор, от второго устройства для обработки данных на третье устройство для обработки данных;

прием на третьем устройстве для обработки данных первого временного идентификатора от первого устройства для обработки данных;

прием на третьем устройстве для обработки данных;

определение на третьем устройстве для обработки данных того, соответствует ли первый временный идентификатор от первого устройства для обработки данных первому временному идентификатору от второго устройства для обработки данных;

отправку третьим устройством для обработки данных на второе устройство для обработки данных указания о том, аутентифицировано ли первое устройство для обработки данных, на основании определения того, соответствует ли первый временный идентификатор от первого устройства для обработки данных первому временному идентификатору от второго устройства для обработки данных;

прием на третьем устройстве для обработки данных второго временного идентификатора от второго устройства для обработки данных;

прием на третьем устройстве для обработки данных первого запроса на аутентификацию;

определение третьим устройством для обработки данных того, соответствует ли второй временный идентификатор от первого устройства для обработки данных второму временному идентификатору от

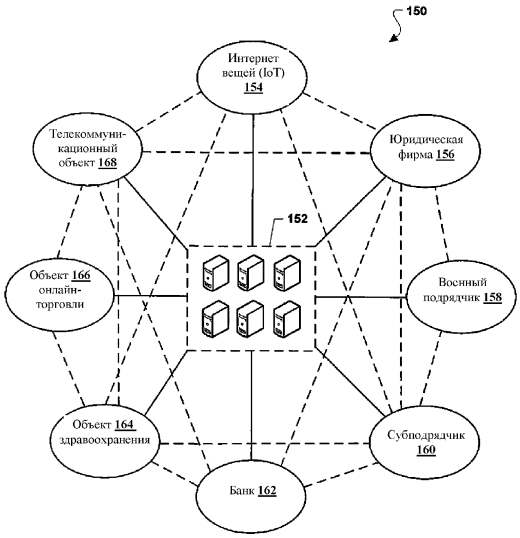
второго устройства для обработки данных;

отправку третьим устройством для обработки данных на первое устройство для обработки данных указания о том, аутентифицировано ли второе устройство для обработки данных, на основании определения того, соответствует ли второй временный идентификатор от первого устройства для обработки данных второму временному идентификатору от второго устройства для обработки данных;

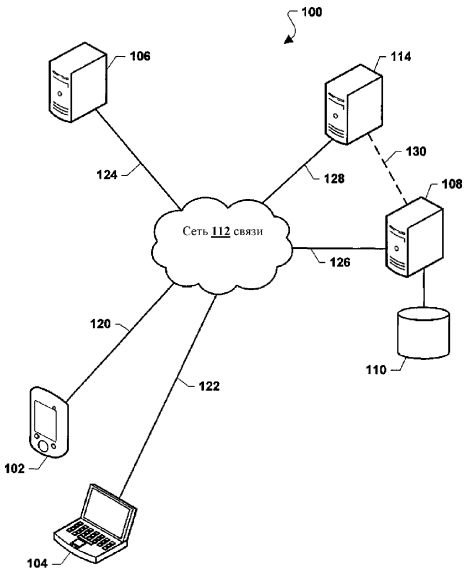
прием на первом устройстве для обработки данных от третьего устройства для обработки данных указания о том, аутентифицировано ли второе устройство для обработки данных; и

прием на втором устройстве для обработки данных от третьего устройства для обработки данных указания о том, аутентифицировано ли первое устройство для обработки данных.

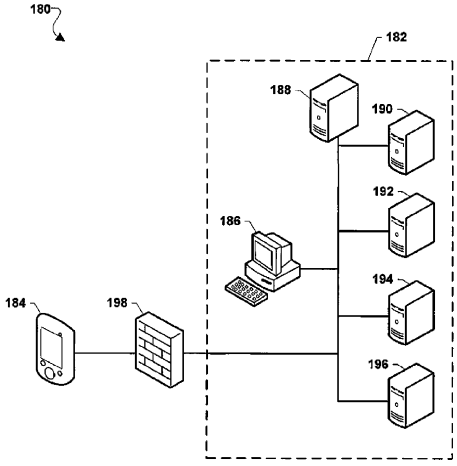
40. Способ по п.39, в котором первое устройство для обработки данных содержит устройство Интернета вещей (IoT).



Фиг. 1A

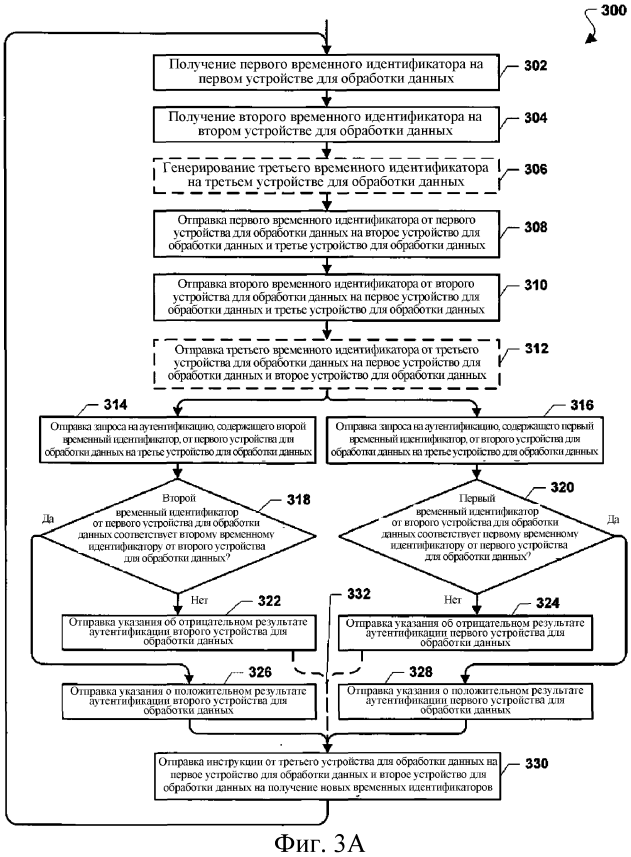


Фиг. 1B

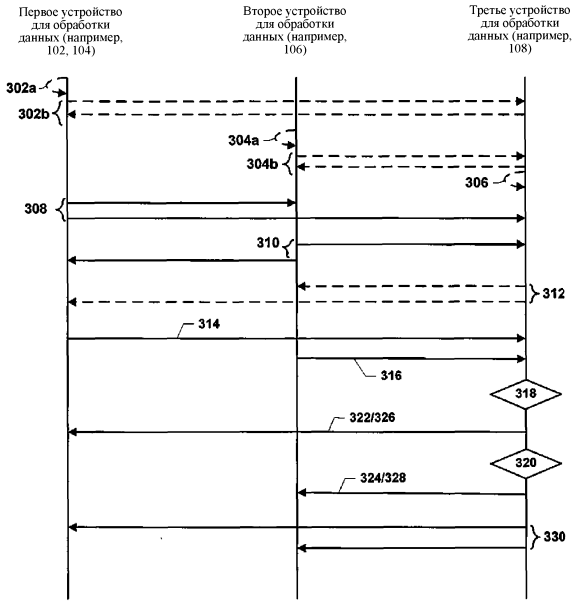


Фиг. 1С

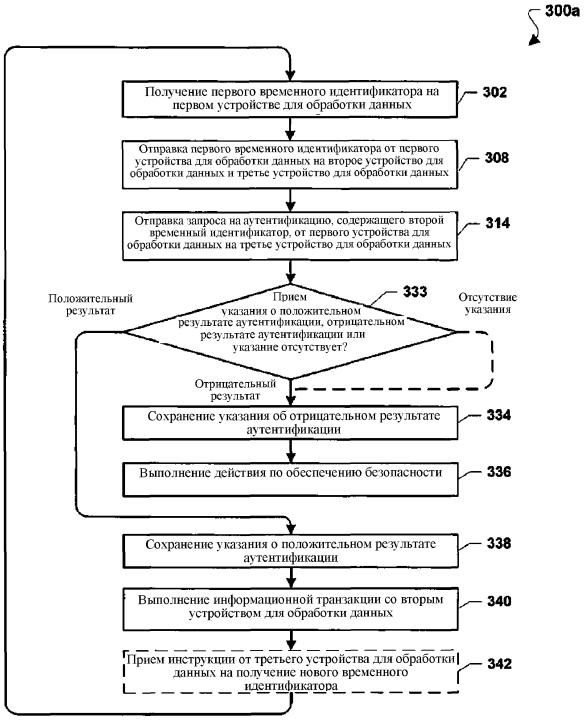
Фиг. 2



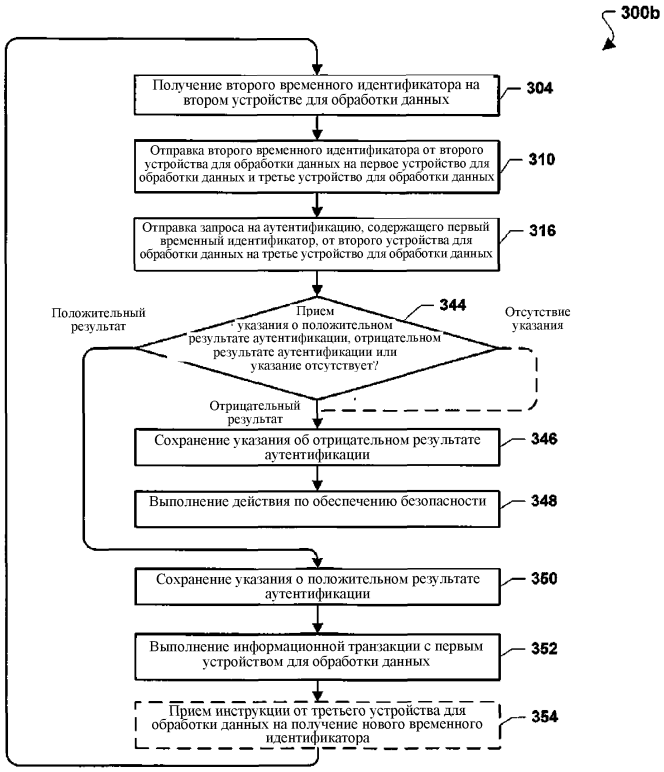
Фиг. 3А


Первое устройство для обработки данных (например, 102, 104)
Второе устройство для обработки данных (например, 106)
Третье устройство для обработки данных (например, 108)
302a
302b
304a
304b
306
308
310
312
314
316
318
322/326
320
324/328
330

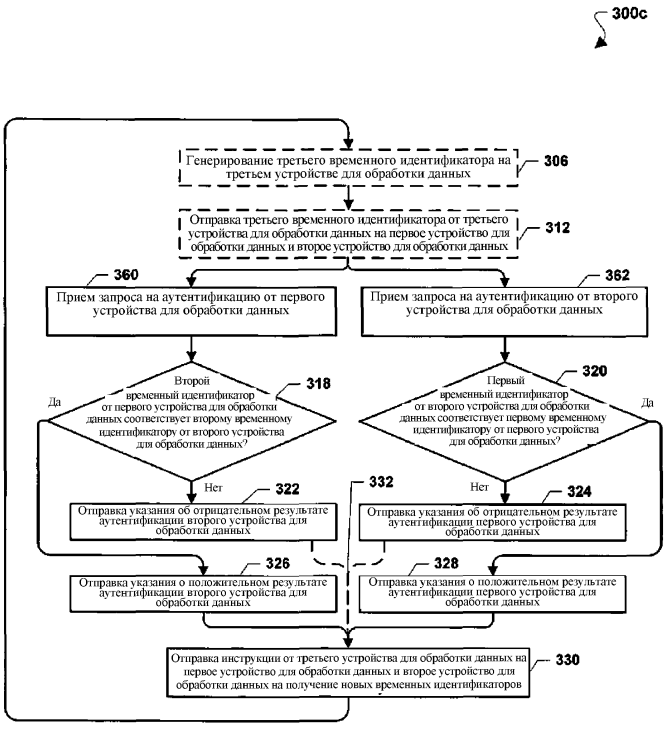
Фиг. 3B


300a
Получение первого временного идентификатора на первом устройстве для обработки данных
302
Отправка первого временного идентификатора от первого устройства для обработки данных на второе устройство для обработки данных и третье устройство для обработки данных
308
Отправка запроса на аутентификацию, содержащего второй временный идентификатор, от первого устройства для обработки данных на третье устройство для обработки данных
314
Положительный результат
Прием указания о положительном результате аутентификации, отрицательном результате аутентификации или указание отсутствует?
333
Отсутствие указания
Отрицательный результат
Сохранение указания об отрицательном результате аутентификации
334
Выполнение действия по обеспечению безопасности
336
Сохранение указания о положительном результате аутентификации
338
Выполнение информационной транзакции со вторым устройством для обработки данных
340
Прием инструкции от третьего устройства для обработки данных на получение нового временного идентификатора
342

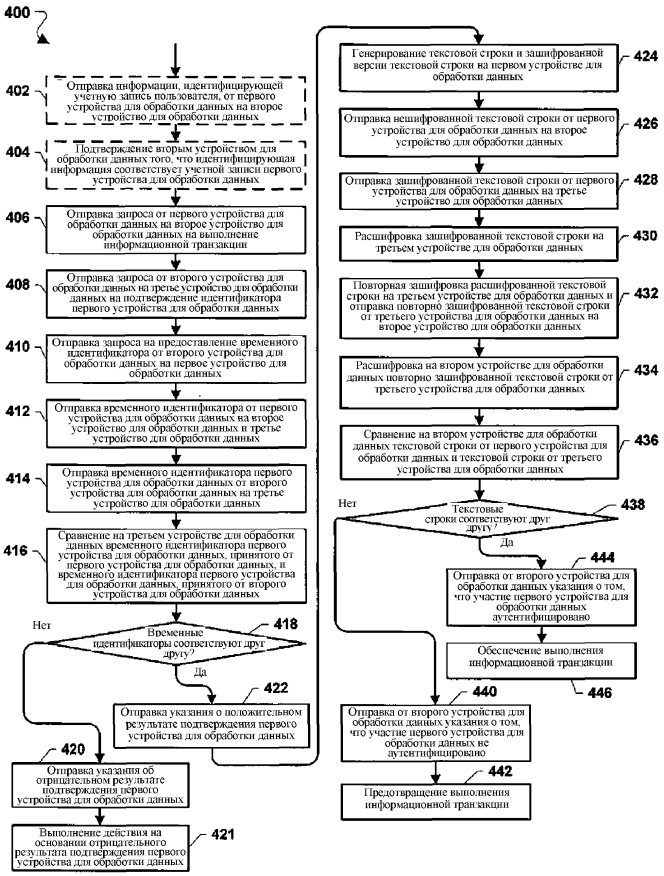
Фиг. 3C


300b
Получение второго временного идентификатора на втором устройстве для обработки данных
304
Отправка второго временного идентификатора от второго устройства для обработки данных на первое устройство для обработки данных и третье устройство для обработки данных
310
Отправка запроса на аутентификацию, содержащего первый временный идентификатор, от второго устройства для обработки данных на третье устройство для обработки данных
316
Прием указания о положительном результате аутентификации, отрицательном результате аутентификации или указание отсутствует?
344
Положительный результат
Отсутствие указания
Отрицательный результат
Сохранение указания об отрицательном результате аутентификации
346
Выполнение действия по обеспечению безопасности
348
Сохранение указания о положительном результате аутентификации
350
Выполнение информационной транзакции с первым устройством для обработки данных
352
Прием инструкции от третьего устройства для обработки данных на получение нового временного идентификатора
354

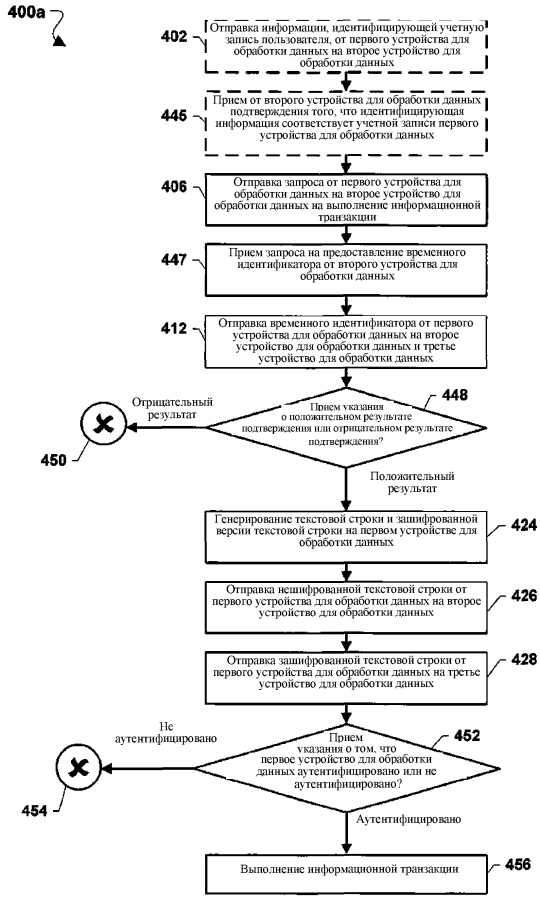
Фиг. 3D


300c
Генерирование третьего временного идентификатора на третьем устройстве для обработки данных
306
Отправка третьего временного идентификатора от третьего устройства для обработки данных на первое устройство для обработки данных и второе устройство для обработки данных
312
360
Прием запроса на аутентификацию от первого устройства для обработки данных
362
Прием запроса на аутентификацию от второго устройства для обработки данных
Второй временный идентификатор от первого устройства для обработки данных соответствует второму временному идентификатору от второго устройства для обработки данных?
318
Да
Первый временный идентификатор от второго устройства для обработки данных соответствует первому временному идентификатору от первого устройства для обработки данных?
320
Да
Нет
322
Отправка указания об отрицательном результате аутентификации второго устройства для обработки данных
332
Нет
324
Отправка указания об отрицательном результате аутентификации первого устройства для обработки данных
326
Отправка указания о положительном результате аутентификации второго устройства для обработки данных
328
Отправка указания о положительном результате аутентификации первого устройства для обработки данных
Отправка инструкции от третьего устройства для обработки данных на первое устройство для обработки данных и второе устройство для обработки данных на получение новых временных идентификаторов
330

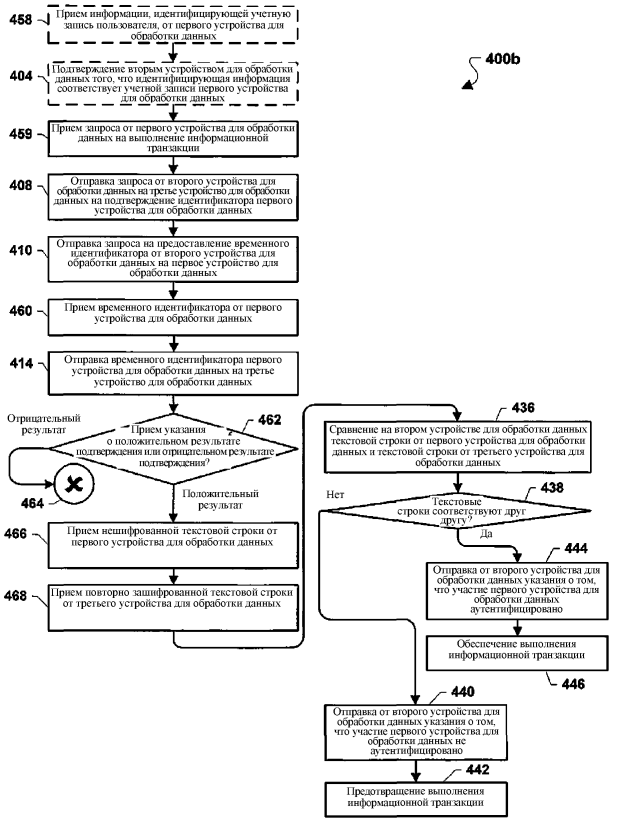
Фиг. 3E


400
402
Отправка информации, идентифицирующей учетную запись пользователя, от первого устройства для обработки данных на второе устройство для обработки данных
404
Подтверждение вторым устройством для обработки данных того, что идентифицирующая информация соответствует учетной записи первого устройства для обработки данных
406
Отправка запроса от первого устройства для обработки данных на второе устройство для обработки данных на выполнение информационной транзакции
408
Отправка запроса от второго устройства для обработки данных на третье устройство для обработки данных на подтверждение идентификатора первого устройства для обработки данных
410
Отправка запроса на предоставление временного идентификатора от второго устройства для обработки данных на первое устройство для обработки данных
412
Отправка временного идентификатора от первого устройства для обработки данных на второе устройство для обработки данных и третье устройство для обработки данных
414
Отправка временного идентификатора первого устройства для обработки данных от второго устройства для обработки данных на третье устройство для обработки данных
416
Сравнение на третьем устройстве для обработки данных временного идентификатора первого устройства для обработки данных, принятого от первого устройства для обработки данных, и временного идентификатора первого устройства для обработки данных, принятого от второго устройства для обработки данных
Нет
418
Временные идентификаторы соответствуют друг другу?
Да
422
Отправка указания о положительном результате подтверждения первого устройства для обработки данных
420
Отправка указания об отрицательном результате подтверждения первого устройства для обработки данных
421
Выполнение действия на основании отрицательного результата подтверждения первого устройства для обработки данных
424
Генерирование текстовой строки и зашифрованной версии текстовой строки на первом устройстве для обработки данных
426
Отправка незашифрованной текстовой строки от первого устройства для обработки данных на второе устройство для обработки данных
428
Отправка зашифрованной текстовой строки от первого устройства для обработки данных на третье устройство для обработки данных
430
Расшифровка зашифрованной текстовой строки на третьем устройстве для обработки данных
432
Повторная зашифровка расшифрованной текстовой строки на третьем устройстве для обработки данных и отправка повторно зашифрованной текстовой строки от третьего устройства для обработки данных на второе устройство для обработки данных
434
Расшифровка на втором устройстве для обработки данных повторно зашифрованной текстовой строки от третьего устройства для обработки данных
436
Сравнение на втором устройстве для обработки данных текстовой строки от первого устройства для обработки данных и текстовой строки от третьего устройства для обработки данных
Нет
438
Текстовые строки соответствуют друг другу?
Да
444
Отправка от второго устройства для обработки данных указания о том, что участие первого устройства для обработки данных аутентифицировано
446
Обеспечение выполнения информационной транзакции
440
Отправка от второго устройства для обработки данных указания о том, что участие первого устройства для обработки данных не аутентифицировано
442
Предотвращение выполнения информационной транзакции

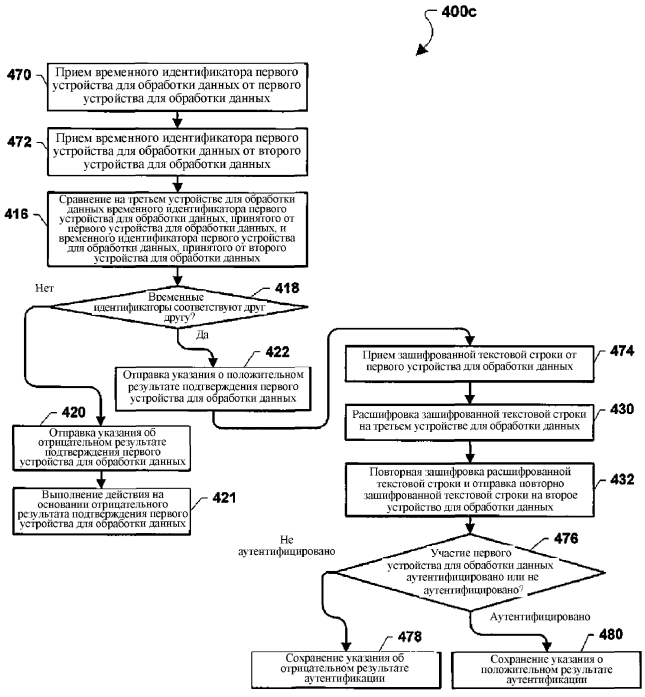
Фиг. 4A


400a
402
Отправка информации, идентифицирующей учетную запись пользователя, от первого устройства для обработки данных на второе устройство для обработки данных
445
Прием от второго устройства для обработки данных подтверждения того, что идентифицирующая информация соответствует учетной записи первого устройства для обработки данных
406
Отправка запроса от первого устройства для обработки данных на второе устройство для обработки данных на выполнение информационной транзакции
447
Прием запроса на предоставление временного идентификатора от второго устройства для обработки данных
412
Отправка временного идентификатора от первого устройства для обработки данных на второе устройство для обработки данных и третье устройство для обработки данных
448
Прием указания о положительном результате подтверждения или отрицательном результате подтверждения?
Отрицательный результат
450
Положительный результат
424
Генерирование текстовой строки и зашифрованной версии текстовой строки на первом устройстве для обработки данных
426
Отправка незашифрованной текстовой строки от первого устройства для обработки данных на второе устройство для обработки данных
428
Отправка зашифрованной текстовой строки от первого устройства для обработки данных на третье устройство для обработки данных
452
Прием указания о том, что первое устройство для обработки данных аутентифицировано или не аутентифицировано?
Не аутентифицировано
454
Аутентифицировано
456
Выполнение информационной транзакции

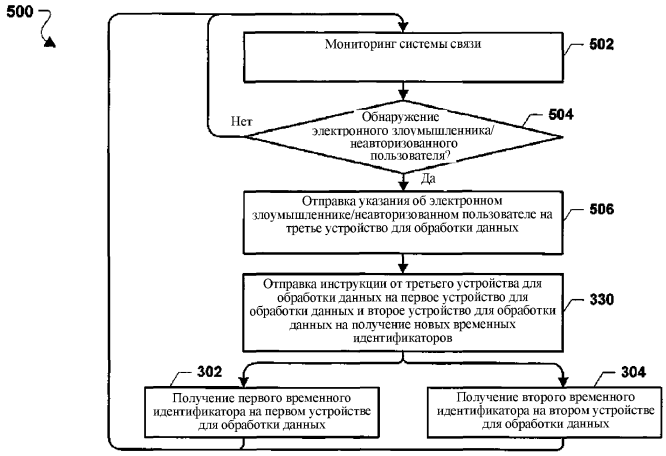
Фиг. 4B


400b
458
Прием информации, идентифицирующей учетную запись пользователя, от первого устройства для обработки данных
404
Подтверждение вторым устройством для обработки данных того, что идентифицирующая информация соответствует учетной записи первого устройства для обработки данных
459
Прием запроса от первого устройства для обработки данных на выполнение информационной транзакции
408
Отправка запроса от второго устройства для обработки данных на третье устройство для обработки данных на подтверждение идентификатора первого устройства для обработки данных
410
Отправка запроса на предоставление временного идентификатора от второго устройства для обработки данных на первое устройство для обработки данных
460
Прием временного идентификатора от первого устройства для обработки данных
414
Отправка временного идентификатора первого устройства для обработки данных на третье устройство для обработки данных
Отрицательный результат
462
Прием указания о положительном результате подтверждения или отрицательном результате подтверждения?
464
Положительный результат
466
Прием нешифрованной текстовой строки от первого устройства для обработки данных
468
Прием повторно зашифрованной текстовой строки от третьего устройства для обработки данных
436
Сравнение на втором устройстве для обработки данных текстовой строки от первого устройства для обработки данных и текстовой строки от третьего устройства для обработки данных
Нет
438
Текстовые строки соответствуют друг другу?
Да
444
Отправка от второго устройства для обработки данных указания о том, что участие первого устройства для обработки данных аутентифицировано
Обеспечение выполнения информационной транзакции
446
440
Отправка от второго устройства для обработки данных указания о том, что участие первого устройства для обработки данных не аутентифицировано
442
Предотвращение выполнения информационной транзакции

Фиг. 4C

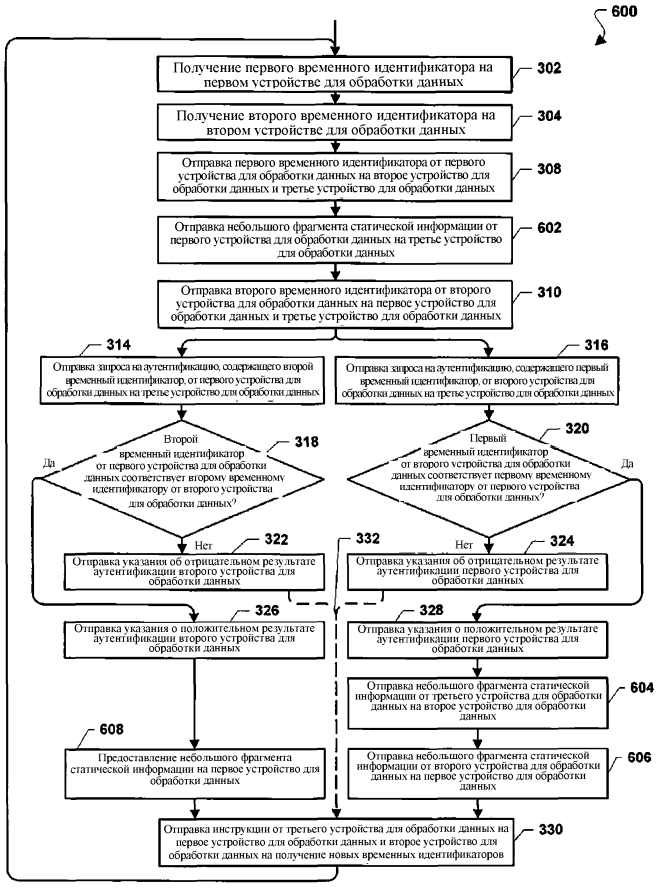

400c
470
Прием временного идентификатора первого устройства для обработки данных от первого устройства для обработки данных
472
Прием временного идентификатора первого устройства для обработки данных от второго устройства для обработки данных
416
Сравнение на третьем устройстве для обработки данных временного идентификатора первого устройства для обработки данных, принятого от первого устройства для обработки данных, и временного идентификатора первого устройства для обработки данных, принятого от второго устройства для обработки данных
Нет
418
Временные идентификаторы соответствуют друг другу?
Да
422
Отправка указания о положительном результате подтверждения первого устройства для обработки данных
420
Отправка указания об отрицательном результате подтверждения первого устройства для обработки данных
Выполнение действия на основании отрицательного результата подтверждения первого устройства для обработки данных
421
474
Прием зашифрованной текстовой строки от первого устройства для обработки данных
430
Расшифровка зашифрованной текстовой строки на третьем устройстве для обработки данных
432
Повторная зашифровка расшифрованной текстовой строки и отправка повторно зашифрованной текстовой строки на второе устройство для обработки данных
Не аутентифицировано
476
Участие первого устройства для обработки данных аутентифицировано или не аутентифицировано?
Аутентифицировано
478
Сохранение указания об отрицательном результате аутентификации
480
Сохранение указания о положительном результате аутентификации

Фиг. 4D

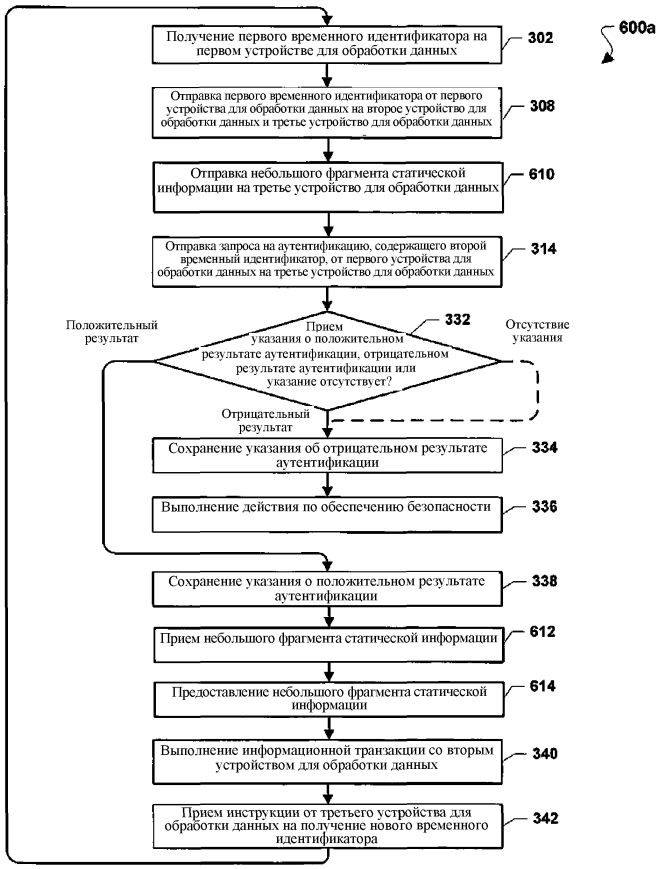


Фиг. 5A

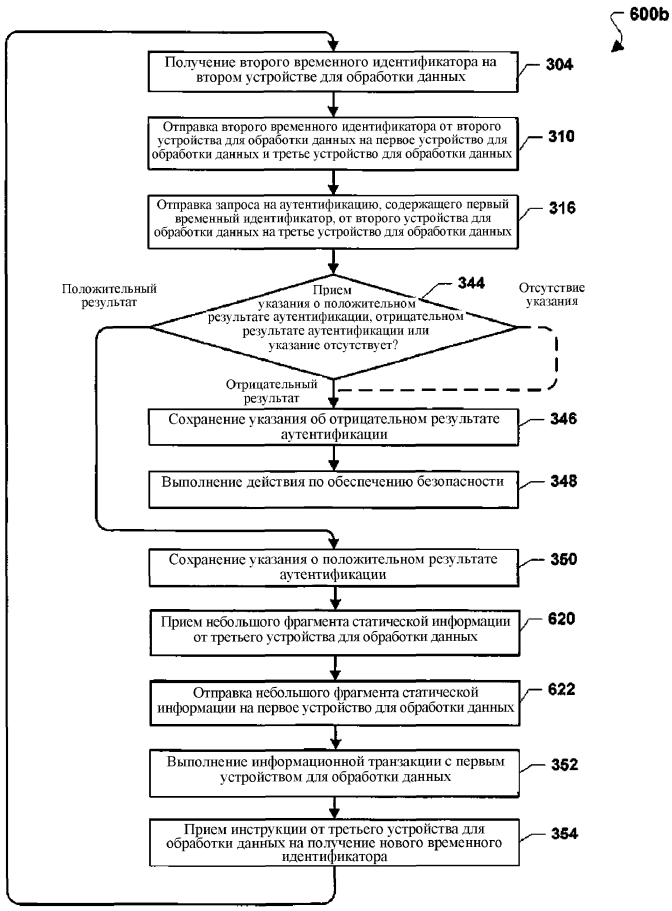
Фиг. 5B



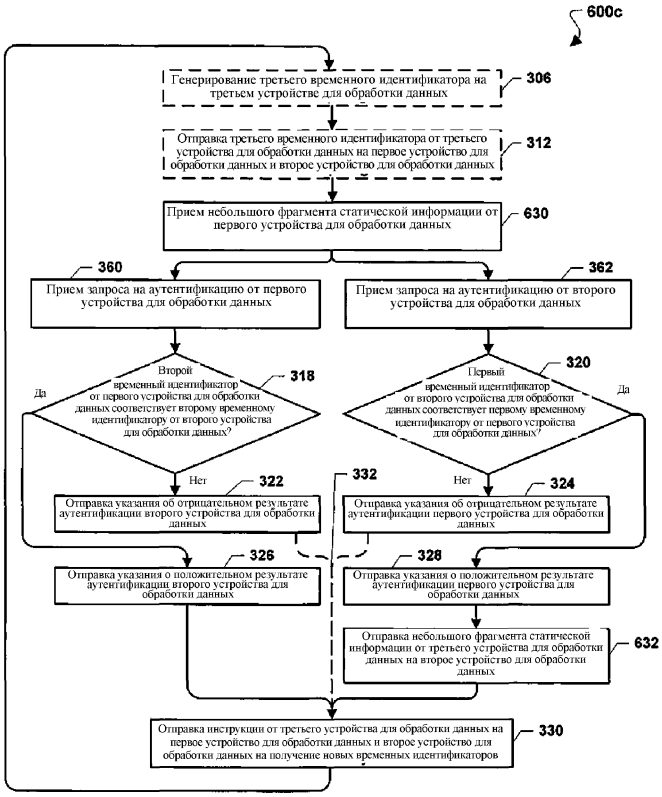
Фиг. 6A


600a
Получение первого временного идентификатора на первом устройстве для обработки данных
302
Отправка первого временного идентификатора от первого устройства для обработки данных на второе устройство для обработки данных и третье устройство для обработки данных
308
Отправка небольшого фрагмента статической информации на третье устройство для обработки данных
610
Отправка запроса на аутентификацию, содержащего второй временный идентификатор, от первого устройства для обработки данных на третье устройство для обработки данных
314
Положительный результат
Прием указания о положительном результате аутентификации, отрицательном результате аутентификации или указание отсутствует?
332
Отсутствие указания
Отрицательный результат
Сохранение указания об отрицательном результате аутентификации
334
Выполнение действия по обеспечению безопасности
336
Сохранение указания о положительном результате аутентификации
338
Прием небольшого фрагмента статической информации
612
Предоставление небольшого фрагмента статической информации
614
Выполнение информационной транзакции со вторым устройством для обработки данных
340
Прием инструкции от третьего устройства для обработки данных на получение нового временного идентификатора
342

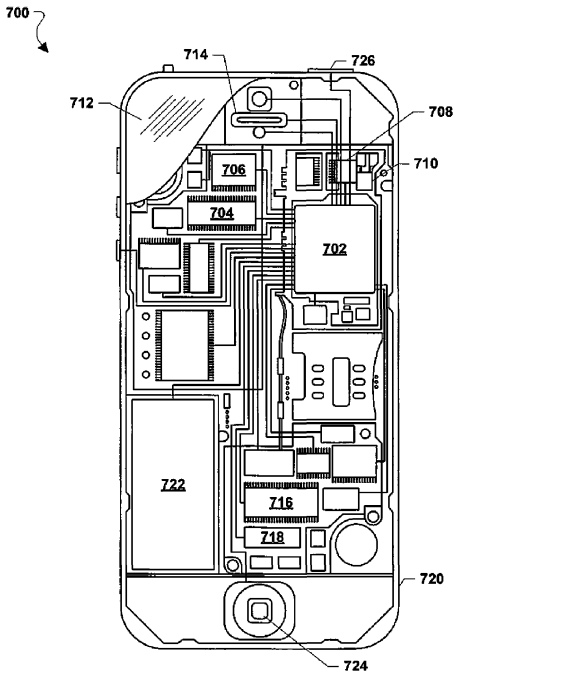
Фиг. 6B


600b
Получение второго временного идентификатора на втором устройстве для обработки данных
304
Отправка второго временного идентификатора от второго устройства для обработки данных на первое устройство для обработки данных и третье устройство для обработки данных
310
Отправка запроса на аутентификацию, содержащего первый временный идентификатор, от второго устройства для обработки данных на третье устройство для обработки данных
316
Положительный результат
Прием указания о положительном результате аутентификации, отрицательном результате аутентификации или указание отсутствует?
344
Отсутствие указания
Отрицательный результат
Сохранение указания об отрицательном результате аутентификации
346
Выполнение действия по обеспечению безопасности
348
Сохранение указания о положительном результате аутентификации
350
Прием небольшого фрагмента статической информации от третьего устройства для обработки данных
620
Отправка небольшого фрагмента статической информации на первое устройство для обработки данных
622
Выполнение информационной транзакции с первым устройством для обработки данных
352
Прием инструкции от третьего устройства для обработки данных на получение нового временного идентификатора
354

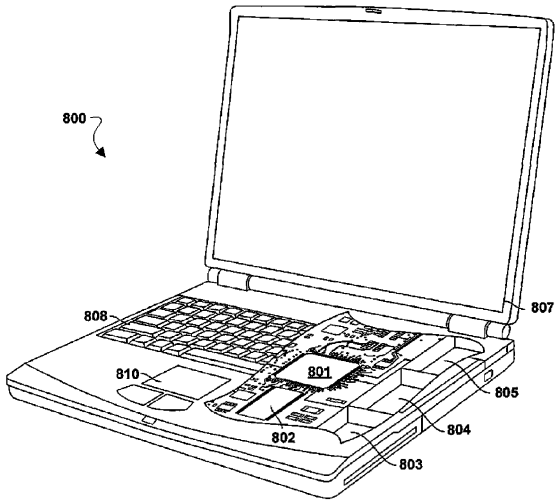
Фиг. 6C


600c
Генерирование третьего временного идентификатора на третьем устройстве для обработки данных
306
Отправка третьего временного идентификатора от третьего устройства для обработки данных на первое устройство для обработки данных и второе устройство для обработки данных
312
Прием небольшого фрагмента статической информации от первого устройства для обработки данных
630
360
Прием запроса на аутентификацию от первого устройства для обработки данных
362
Прием запроса на аутентификацию от второго устройства для обработки данных
Второй временный идентификатор от первого устройства для обработки данных соответствует второму временному идентификатору от второго устройства для обработки данных?
318
Да
Нет
Первый временный идентификатор от второго устройства для обработки данных соответствует первому временному идентификатору от первого устройства для обработки данных?
320
Да
Нет
322
Отправка указания об отрицательном результате аутентификации второго устройства для обработки данных
332
324
Отправка указания об отрицательном результате аутентификации первого устройства для обработки данных
326
Отправка указания о положительном результате аутентификации второго устройства для обработки данных
328
Отправка указания о положительном результате аутентификации первого устройства для обработки данных
Отправка небольшого фрагмента статической информации от третьего устройства для обработки данных на второе устройство для обработки данных
632
Отправка инструкции от третьего устройства для обработки данных на первое устройство для обработки данных и второе устройство для обработки данных на получение новых временных идентификаторов
330

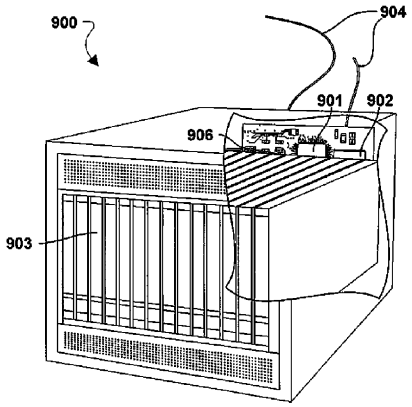
Фиг. 6D


700
714
726
712
708
710
706
704
702
722
716
718
720
724

Фиг. 7



Фиг. 8



Фиг. 9