

(19)



**Евразийское
патентное
ведомство**

(11) **036443**(13) **B1**

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2020.11.11

(21) Номер заявки
201691377

(22) Дата подачи заявки
2015.01.09

(51) Int. Cl. *H04L 29/06* (2006.01)
G06Q 20/20 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/40 (2012.01)
G06F 21/62 (2013.01)

(54) СИСТЕМА И СПОСОБ ПЕРЕДАЧИ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ

(31) **14150856.4**

(32) **2014.01.10**

(33) **EP**

(43) **2017.03.31**

(86) **PCT/EP2015/050354**

(87) **WO 2015/104387 2015.07.16**

(71)(73) Заявитель и патентовладелец:
ПРАЙВИТИ ПТЕ. ЛТД. (SG)

(72) Изобретатель:
Барри Джерард (IE), Барри Деклан (SG)

(74) Представитель:
Носырева Е.Л. (RU)

(56) US-A1-2013246203
WO-A1-2004049621
WO-A1-2013034192

(57) Система и способ для выполнения транзакций, включающих передачу идентификационных данных, связанных с организацией или лицом, известным как предъявитель, в разрешенный пункт назначения, известный как конечная точка (110) сети, после запроса от приемщика, при этом поддерживая секретность в указанных идентификационных данных. Система содержит устройства (108) предъявления и устройства (109) приема, которые обмениваются данными с управляющим сервером (101). Управляющий сервер принимает сообщение от устройств приема и предъявления, которое содержит секретный ключ, являющийся уникальным для лица или предъявителя, идентификаторы предъявителя и общий ключ, при этом если сообщения соответствуют друг другу, разрешается выдача идентификационных данных, характерных для идентификатора предъявителя, на известную конечную точку сети.

B1**036443****036443****B1**

Область техники, к которой относится изобретение

Настоящее изобретение относится к области информационно-коммуникационной технологии, секретности обмена данными, защита которой доверена информационно-коммуникационной технологии, а также сохранению и защите секретности, имеющей приоритетное значение в идентификационных данных, передаваемых с помощью информационно-коммуникационной технологии. Секретность относится к обладанию любой информацией или участию в использовании любой информации, которая относится к организации, или любого набора идентификационных данных, связанных с организацией и любым конкретным лицом. В частности, настоящее изобретение относится, но без ограничения, к разрешенной выдаче данных, содержащих наборы частных личных сведений и контролируемых идентификационных данных, которые сторона, которой принадлежит набор идентификационных данных, может захотеть позволить и разрешить конфиденциально выдать защищенным и надежным способом, при этом обеспечивая непрерывное сохранение и поддержание конфиденциальности и приватности личных сведений и контролируемых идентификационных данных в различных целях. Контролируемые идентификационные данные относятся к такой информации, которая связывает владельца/эмитента контролируемых идентификационных данных и держателя/обладателя контролируемых идентификационных данных.

Предпосылки создания изобретения

В современном обществе люди связаны с огромным количеством личных данных. Некоторые примеры таких личных данные включают без ограничения имя, адрес, дату рождения, национальность, номер социального страхования, номер паспорта, номер водительского удостоверения, членский номер (определенной организации), девичью фамилию (если имеется), девичью фамилию матери, информацию о работодателе, номер банковского счета, номер кредитной карты и т.д. Указанные личные данные используются множеством способов, в случае когда лица взаимодействуют с другими лицами и организациями. Большое количество этих случаев взаимодействия сильно зависит от точности набора данных, который как является характерным для лица, так и является необходимым для рассматриваемого взаимодействия. Соответственно, поскольку каждый такой набор данных (далее называемый как "набор идентификационных данных") как является характерным для лица, так и является необходимым для взаимодействия, он является конфиденциальной информацией, которую желательно хранить в состоянии секретности. Информация представляет собой конфиденциальные (и желательно хранящиеся в состоянии секретности) дополнительные соответствующие данные, такие как данные, относящиеся к дополнительным средствам защиты, например секретному ключу, связанному с указанным документом. Следует понимать, что даже если необходимо выдать набор идентификационных данных из записи, может быть необходимым предотвратить разглашение связанных данных, особенно когда они относятся к дополнительным средствам защиты.

Такие реестры записей обычно заполняются следующим образом. Набор идентификационных данных, относящийся к предъявителю, предоставляется контроллеру и набор идентификационных данных проверяется и признается действительным. После проверки и признания действительности набора идентификационных данных создается документ, содержащий набор идентификационных данных, и этот набор идентификационных данных предоставляется предъявителю. Набор идентификационных данных также вводится в новую запись в реестре записей и обычно дополняется любыми данными, относящимися к соответствующему документу (например, серийным номером и т.д.), и любыми другими соответствующими данными (такими как дополнительные данные средства защиты, включая без ограничения биометрические характеристики и т.д.).

Были разработаны способы представления наборов идентификационных данных в такие индивидуальные документы. Ранее такие данные могли быть нанесены краской, напечатаны или нанесены в виде этикетки на выданный документ. Впоследствии такие данные могли быть выполнены тиснением или гравировкой, или закодированы, или встроены в выданный документ. В последнее время в качестве документов использовались машиночитаемые носители (такие как магнитные полосы или чипы), причем соответствующие наборы идентификационных данных хранились на указанных носителях в электронном виде. Формат многих документов (и формат, в котором на них хранятся наборы идентификационных данных) регулируется Международной организацией по стандартизации. Например, стандарт ISO 7501 устанавливает формат машиночитаемых проездных документов; стандарты ISO 7810 и ISO 7811 устанавливают формат идентификационных карт; и стандарты ISO 7812 и ISO 7816 устанавливают способ, посредством которого карты могут быть предоставлены от различных эмитентов.

Несмотря на преимущества при предоставлении документов, содержащих наборы идентификационных данных предъявителя, остается опасность подделки. Остается необходимость как в получении возможности проверки того, что предъявитель, имеющий документ, содержащий набор идентификационных данных, является действительным/настоящим предъявителем (т.е. что документ не был украден или скопирован и, следовательно, не используется мошенническим путем), так и проверки того, что предъявляемый документ, содержащий набор идентификационных данных, является на самом деле подлинным (т.е. что идентификационные данные являются точными и что документ не является полной подделкой). Это представляет собой проблему, вызывающую все большую озабоченность, поскольку владельцы таких документов выдают свои наборы идентификационных данных с увеличивающейся час-

тотой. Хотя наборы идентификационных данных изначально хранятся в среде конфиденциальности/приватности, предусмотренной между предъявителями наборов идентификационных данных и их контролерами, данная среда конфиденциальности/приватности находится под угрозой каждый раз, когда набор идентификационных данных выдают во время обмена данными с третьей стороной. Хотя улучшения безопасности средств, с помощью которых происходит выдача наборов идентификационных данных, направлены на поддержание этой среды конфиденциальности/приватности, в них все еще остаются уязвимые места.

Например, даже с появлением автоматических систем считывания паспортных документов, когда пассажир предъявляет свой паспорт любому сотруднику контрольно-пропускного пункта или любому представителю органов пограничного контроля ("приемщик"), контролируемые идентификационные данные на выданном документе видит и обрабатывает приемщик перед и после сбора контролируемых идентификационных данных считывающим устройством. Если в нарушение политики конфиденциальности указанные идентификационные данные после просмотра скопированы и переданы кому-либо приемщиком, а не только собраны и обработаны, ставится под угрозу состояние секретности, в котором изначально находились идентификационные данные паспортного документа. Аналогичные уязвимые места существуют и у других документов, для которых были разработаны автоматические системы сбора идентификационных данных, такие как водительские удостоверения, карты постоянного покупателя/членские карты и платежные карты.

Остается необходимость в улучшенных способах и системах, с помощью которых предъявители смогут предъявлять наборы идентификационных данных во время обмена данными с другими лицами или организациями таким образом, который гарантирует как подлинность набора идентификационных данных, так и подлинность предъявителя, имеющего набор идентификационных данных. Было бы очень желательно предоставить способы и системы, которые обеспечивают среду полной конфиденциальности/приватности для наборов идентификационных данных, когда они раскрываются. Было бы крайне предпочтительно, чтобы любые такие улучшенные способы и системы обладали обратной совместимостью с существующими способами и системами, которые повсеместно используются, чтобы улучшенные способы и системы могли быть введены плавно и постепенно. Было бы очень предпочтительно, если бы была устранена необходимость в дорогостоящих и длительных переходах на новые системы и способы. Кроме того, было бы предпочтительно, чтобы новые улучшенные способы и системы были адаптируемыми, чтобы они могли подходить для использования множества различных наборов идентификационных данных посредством одной системы и способа.

В документе US-A-2013/0246203 описано осуществление платежных операций, в которых снижена вероятность подделки. Платежные идентификационные данные покупателя не предоставляются продавцу и к ним не может быть получен доступ для использования в платежной операции, кроме случаев, когда запрос на доступ получают от авторизованного устройства, назначенного покупателем. В одном варианте осуществления авторизованное устройство представляет собой мобильный телефон.

В документе WO-A-2004/049621 описана система установления подлинности, в которой первый терминал обменивается данными с организатором по первому каналу связи, а второй терминал обменивается данными с оператором по второму каналу связи, причем организатор и оператор могут обмениваться данными друг с другом. Идентификационные данные не предоставляются на первый терминал оператором, организатором или вторым терминалом, при этом идентификационные данные первого терминала не предоставляются на второй терминал оператором, организатором или первым терминалом, таким образом, обмен данными между первым терминалом и организатором и между вторым терминалом и оператором не содержит данные, относящиеся к идентификационной информации пользователя.

В документе WO-A-2013/034192 описан способ проверки достоверности электронной транзакции, в котором идентификационные данные передают с мобильного телефона на торговый терминал, при этом их подлинность должна быть проверена с помощью PIN-кода, предоставленного на сервер во время голосового телефонного вызова.

Сущность изобретения

Один аспект настоящего изобретения относится к системе для обеспечения передачи по меньшей мере одного набора контролируемых идентификационных данных, связанных с предъявителем, на конечную точку сети, при этом поддерживая секретность, имеющую приоритетное значение в указанных контролируемых идентификационных данных, связанных с предъявителем, при этом система содержит по меньшей мере одно устройство приема, по меньшей мере одно устройство предъявления, по меньшей мере одну конечную точку сети и по меньшей мере один сервер, причем один из указанных серверов содержит одну или более записей. Каждая запись относится к определенному предъявителю, содержит идентификатор предъявителя и секретный ключ, соответствующий каждому идентификатору предъявителя, и связана по меньшей мере с одной отметкой, относящейся к набору контролируемых идентификационных данных, связанных с предъявителем. Каждая отметка относится по меньшей мере к одному набору идентификационных данных, связанных с определенным предъявителем. Каждая отметка также может относиться по меньшей мере к одному условному названию, причем каждое условное название соответственно связано с одним из указанных наборов идентификационных данных. Каждая конечная

точка сети представляет собой назначенного получателя типа контролируемых идентификационных данных, связанных с предъявителями, причем указанная конечная точка представляет собой либо устройство приема, либо устройство назначенной третьей стороны, сопряженное с устройством приема; причем обеспечение передачи по меньшей мере одного набора контролируемых идентификационных данных, связанных с предъявителем, осуществляют в контексте взаимодействия между предъявляющей стороной взаимодействия и принимающей стороной взаимодействия; и причем набор идентификационных данных, к которому относится разрешение, связан с предъявляющей стороной взаимодействия. Один из указанных серверов выполняет функцию управляющего сервера, дополнительно выполненного с возможностью (а) получения сообщения от устройства приема, далее называемого как сообщение устройства приема, причем указанное сообщение содержит секретный ключ, относящийся к предъявителю, и одноразовый общий ключ; (б) получения сообщения от устройства предъявления, далее называемого как сообщение устройства предъявления, причем указанное сообщение содержит идентификатор предъявителя, относящийся к предъявителю, и одноразовый общий ключ; (с) поиска соответствия между одноразовым общим ключом, содержащимся в сообщении устройства приема, и соответствующим одноразовым общим ключом, содержащимся в сообщении устройства предъявления; (d) инициации поиска целевой записи путем связывания секретного ключа, содержащегося в указанном сообщении устройства приема, и идентификатором предъявителя, содержащимся в указанном сообщении устройства предъявления, причем оба указанных сообщения содержат одинаковый общий ключ; (е) выполнения поиска указанной целевой записи, которая содержит как указанный секретный ключ, так и указанный идентификатор предъявителя; (f) идентификации отметки, связанной с указанной целевой записью, причем указанная отметка относится к набору контролируемых идентификационных данных, связанных с предъявителем; (g) обеспечения извлечения указанного набора идентификационных данных, относящихся к указанной отметке, и обеспечения выдачи указанного набора идентификационных данных на указанную конечную точку сети, причем указанная конечная точка является разрешенным получателем набора контролируемых идентификационных данных, связанных с указанным предъявителем, и указанная конечная точка представляет собой либо устройство приема, либо устройство назначенной третьей стороны, сопряженное с устройством приема.

Другой аспект настоящего изобретения относится к способу обеспечения передачи по меньшей мере одного набора контролируемых идентификационных данных, связанных с предъявителем, от сервера на конечную точку сети, при этом поддерживая секретность, имеющую приоритетное значение в указанных контролируемых идентификационных данных, связанных с предъявителем; и причем сервер содержит одну или более записей, причем каждая запись относится к предъявителю (определенная сторона, зарегистрированная с помощью сервера как предъявитель и/или как приемщик), и каждая запись содержит идентификатор предъявителя (и/или идентификатор приемщика) и секретный ключ (предъявителя и/или приемщика), соответствующий указанному идентификатору предъявителя, и каждая запись связана с отметкой, относящейся к набору контролируемых идентификационных данных (соответствующих указанной стороне), связанных с указанным предъявителем; причем способ включает (а) предоставление доступа устройством приема к одноразовому общему ключу для предъявляющей стороны взаимодействия; (б) получение секретного ключа (предъявителя), относящегося к предъявляющей стороне взаимодействия, на устройстве приема, причем указанный секретный ключ (предъявителя) вводит на устройстве приема предъявляющая сторона взаимодействия; (с) передачу сообщения устройства приема от устройства приема по меньшей мере на один из серверов, причем указанное сообщение устройства приема содержит одноразовый общий ключ и секретный ключ (предъявителя); (d) получение одноразового общего ключа на устройстве предъявления предъявляющей стороны взаимодействия; (е) извлечение идентификатора предъявителя, относящегося к предъявляющей стороне взаимодействия, из места хранения на устройстве предъявления, осуществляемое на устройстве предъявления; и (f) передачу сообщения устройства предъявления на указанный сервер, осуществляемую на устройстве предъявления, причем указанное сообщение устройства предъявления содержит одноразовый общий ключ и идентификатор предъявителя, причем (g) после получения указанного сообщения устройства приема и указанного сообщения устройства предъявления обработку сообщений на сервере, чтобы убедиться в наличии разрешения на передачу набора контролируемых идентификационных данных, связанных с предъявителем, тем самым разрешая его извлечение из сервера и, таким образом, разрешая его выдачу на конечную точку сети, причем указанная конечная точка является разрешенным получателем, и указанная конечная точка является либо устройством приема, либо устройством назначенной третьей стороны, сопряженным с устройством приема.

В одном аспекте настоящего изобретения все наборы идентификационных данных, связанные с предъявителем (или условные названия, соответствующие наборам идентификационных данных), могут находиться в виде отметок в указанной записи.

В другом аспекте настоящего изобретения все наборы идентификационных данных, связанные с предъявителем (и соответствующие условные названия), могут находиться в виде отдельных отметок на другом сервере, выполненном с возможностью связи с управляющим сервером. Альтернативно, некоторые наборы идентификационных данных, связанные с предъявителем, и соответствующие условные на-

звания могут находиться в виде отметок в указанной записи, при этом другие могут находиться в виде отдельных отметок на указанном сервере или отдельных отметок на других серверах.

Сообщение устройства приема может быть передано на указанный сервер по первому каналу связи, а сообщение устройства предъявления может быть передано на указанный сервер по второму каналу связи.

В одном аспекте настоящего изобретения одноразовый общий ключ может быть сгенерирован на сервере и передан на устройство приема перед предоставлением доступа к указанному одноразовому общему ключу для предъявляющей стороны взаимодействия и/или устройства предъявления.

В другом аспекте настоящего изобретения одноразовый общий ключ может быть сгенерирован на устройстве приема перед предоставлением доступа к указанному одноразовому общему ключу для предъявляющей стороны взаимодействия и/или устройства предъявления.

Копия одноразового общего ключа может быть передана от устройства приема на устройство предъявления с помощью беспроводной технологии, причем беспроводная технология необязательно выбрана из группы, содержащей Wi-Fi, Bluetooth, NFC или RFID.

В одном аспекте настоящего изобретения период достоверности может быть назначен сообщению устройства приема и сообщениям устройства предъявления и/или общему ключу. Это обеспечивает то, что если сообщение устройства приема не соответствует сообщению устройства предъявления, как описано ниже, в пределах определенного интервала времени (периода достоверности), то такая передача прекращается и, таким образом, завершается, что делает дальнейшие процессы лишними. Если такая передача прекращается и завершается, делая дальнейшие процессы лишними, данные, относящиеся к сообщению, могут быть удалены, высвобождая ресурсы для обработки других сообщений. Если сообщения генерируют, передают или получают, и они содержат общие ключи, имеющие период достоверности, период достоверности может обеспечивать возможность использования более коротких и менее сложных общих ключей, поскольку таким образом становится целесообразным повторное использование общего ключа. После истечения периода достоверности общего ключа тот же общий ключ может быть повторно использован в последующей итерации способа.

В одном аспекте настоящего изобретения к копии одноразового общего ключа может быть предоставлен доступ для предъявляющей стороны взаимодействия и/или устройства предъявления посредством экрана, входящего в состав устройства приема, или на распечатке из устройства приема, при этом либо (а) к копии одноразового общего ключа предоставляют доступ в машиночитаемом формате, например UTF-8, и копию одноразового общего ключа принимают на периферийном устройстве предъявления путем ввода от предъявляющей стороны взаимодействия, и/или принимающей стороны взаимодействия, и/или устройства приема; либо (б) копия одноразового общего ключа находится в QR-коде, и копию одноразового общего ключа принимают на устройстве предъявления посредством функции камеры, находящейся в устройстве предъявления, которая используется для захвата QR-кода и извлечения копии одноразового общего ключа.

Сообщение устройства приема может дополнительно содержать один или более предварительно определенных вспомогательных параметров, и сообщение устройства предъявления также может дополнительно содержать указанный один или более предварительно определенных вспомогательных параметров. Возможен вариант, при котором эти вспомогательные параметры также необязательно должны соответствовать друг другу, как будет описано ниже, перед успешным подтверждением для инициации и выполнения поиска каких-либо целевых записей. Это дополнительное условие соответствия в процессе подтверждения, в случае обязательного использования в дополнение к общему ключу, дополнительно улучшает способ, поскольку вводит дополнительный критерий в процесс поиска соответствия между сообщением устройства приема и сообщением устройства предъявления. Предварительно определенный вспомогательный параметр может представлять собой код, согласованный между принимающей стороной взаимодействия и предъявляющей стороной взаимодействия, или может представлять собой значение, относящееся к взаимодействию между предъявляющей стороной взаимодействия и принимающей стороной взаимодействия, например значение запланированной транзакции.

Если период достоверности назначен одноразовому общему ключу, указанный общий ключ может быть уникальным в течение длительности его периода достоверности.

Другой аспект настоящего изобретения относится к способу обеспечения передачи по меньшей мере одного набора контролируемых идентификационных данных, связанных с предъявителем, с сервера на конечную точку сети, при этом поддерживая секретность, имеющую приоритетное значение в наборе контролируемых идентификационных данных, связанных с предъявителем, причем разрешение включает сообщение устройства приема, содержащее общий ключ и секретный ключ предъявителя, и сообщение устройства предъявления, содержащее общий ключ и идентификатор предъявителя, причем способ включает (а) получение на сервере сообщения устройства приема; (б) получение на сервере сообщения устройства предъявления; (с) поиск на сервере соответствия между одноразовым общим ключом, содержащимся в сообщении устройства приема, и соответствующим одноразовым общим ключом, содержащимся в сообщении устройства предъявления, (d) инициацию поиска на сервере целевой записи путем связывания секретного ключа (предъявителя), содержащегося в сообщении устройства приема, и иден-

тификатора предъявителя, содержащегося в сообщении устройства предъявления, причем оба указанных сообщения содержат одинаковый общий ключ; (е) выполнение поиска на сервере целевой записи, содержащей как указанный секретный ключ (предъявителя), так и указанный идентификатор предъявителя; (ф) если целевая запись идентифицирована, идентификацию на сервере отметки, связанной с указанной целевой записью, причем указанная отметка относится к контролируемым идентификационным данным, связанным с предъявителем; (г) обеспечение извлечения из сервера указанного набора идентификационных данных, идентифицированных указанной отметкой, связанной с целевой записью, и обеспечение выдачи указанного набора идентификационных данных на указанную конечную точку сети, причем указанная конечная точка является разрешенным получателем набора контролируемых идентификационных данных, связанных с предъявителем, и указанная конечная точка представляет собой либо устройство приема, либо устройство назначенной третьей стороны, сопряженное с устройством приема.

Целевая запись на указанном сервере также может дополнительно содержать условное название, соответствующее указанной отметке, относящейся к каждому набору идентификационных данных, связанных с предъявителем, и сообщение устройства предъявления может дополнительно содержать копию условного названия, выбранную из списка условных названий, составленного на устройстве предъявления, причем на этапе выполнения поиска целевой записи, содержащей такой же идентификатор предъявителя и секретный ключ, также используют копию условного названия, содержащегося в сообщении устройства предъявления, для поиска целевой записи, содержащей такое же указанное условное название в дополнение к такому же идентификатору предъявителя и секретному ключу.

Отметка, относящаяся к набору идентификационных данных, связанных с предъявителем, может находиться в указанной целевой записи на указанном управляющем сервере, выполненном с возможностью обеспечения извлечения и выдачи набора идентификационных данных, связанных с предъявителем, причем этапы извлечения набора идентификационных данных, связанных с предъявителем, и выдача набора идентификационных данных, связанных с предъявителем, выполняют на указанном управляющем сервере, выполненном с возможностью извлечения и выдачи набора идентификационных данных, связанных с предъявителем.

Набор идентификационных данных, связанных с предъявителем, может находиться в отдельных отметках на другом сервере, отличном от указанного управляющего сервера, выполненном с возможностью обеспечения извлечения и выдачи набора идентификационных данных, связанных с предъявителем, причем отдельная отметка связана с целевой записью, при этом этапы извлечения и выдачи набора идентификационных данных выполняют либо на указанном управляющем сервере, выполненном с возможностью обеспечения извлечения и выдачи набора идентификационных данных, связанных с предъявителем, либо на указанном другом сервере, отличном от управляющего сервера, выполненном с возможностью обеспечения извлечения и выдачи набора идентификационных данных, связанных с предъявителем.

Период достоверности может быть назначен сообщению устройства приема и/или сообщению устройства предъявления, и/или общему ключу, содержащемуся в сообщении устройства приема и/или в сообщении устройства предъявления, при этом этап поиска соответствия между общим ключом, содержащимся в сообщении устройства приема, и общим ключом, содержащимся в сообщении устройства предъявления, дополнительно включает установление того, истек ли период достоверности. Это обеспечивает то, что если сообщение устройства приема не соответствует сообщению устройства предъявления, как описано ниже, в пределах определенного интервала времени (периода достоверности), то такое взаимодействие/уведомление/передача прекращается и, таким образом, завершается, что делает дальнейшие процессы лишними. Если любой период достоверности истекает и завершается, делая дальнейшие процессы лишними, данные, относящиеся к сообщению, могут быть удалены, высвобождая ресурсы для обработки других сообщений. Если какие-либо сообщения генерируют/передают/получают и они содержат общие ключи, имеющие период достоверности, период достоверности может обеспечивать возможность использования более коротких и менее сложных общих ключей, поскольку таким образом становится целесообразным повторное использование общего ключа. После истечения периода достоверности общего ключа тот же общий ключ может быть повторно использован в последующей итерации способа.

Если период достоверности назначен общему ключу, указанный общий ключ может быть уникальным в течение длительности его периода достоверности.

Сообщение устройства приема может дополнительно содержать один или более предварительно определенных вспомогательных параметров, и сообщение устройства предъявления также может дополнительно содержать указанный один или более предварительно определенных вспомогательных параметров, причем этап поиска соответствия между общими ключами дополнительно включает этап поиска соответствия между предварительно определенным вспомогательным параметром, содержащимся в сообщении устройства приема, и соответствующим предварительно определенным вспомогательным параметром, содержащимся в сообщении устройства предъявления.

Дополнительный аспект настоящего изобретения относится к способу обеспечения передачи набора контролируемых идентификационных данных, связанных с предъявителем, от сервера на конечную точку сети, при этом поддерживая секретность, имеющую приоритетное значение в идентификационных

данных, связанных с предъявителем, причем разрешение выполняется/представляется в соответствии с любым из аспектов настоящего изобретения, описанных выше, причем способ включает (a) получение на сервере сообщения устройства приема; (b) получение на сервере сообщения устройства предъявления; (c) поиск на сервере соответствия между одноразовым общим ключом, содержащимся в сообщении устройства приема, и соответствующим одноразовым общим ключом, содержащимся в сообщении предъявляющей стороны взаимодействия (и, таким образом, установление соответствия между указанным сообщением устройства приема и указанным сообщением устройства предъявления); (d) инициацию на сервере поиска целевой записи путем связывания секретного ключа, содержащегося в сообщении устройства приема, и идентификатора предъявителя, содержащегося в сообщении устройства предъявления; (e) выполнение на сервере поиска целевой записи, содержащей как указанный секретный ключ, так и указанный идентификатор предъявителя; (f) если целевая запись идентифицирована, идентификацию отметки, относящейся к набору идентификационных данных, связанных с предъявителем и соответствующих ему; (g) если набор идентификационных данных, связанных с предъявителем, идентифицирован, обеспечение извлечения из сервера набора идентификационных данных, связанных с предъявителем, и обеспечение выдачи указанного набора идентификационных данных, связанных с предъявителем, на указанную конечную точку сети, причем указанная конечная точка является разрешенным получателем набора идентификационных данных, связанных с предъявителем, и указанная конечная точка представляет собой либо устройство приема, либо устройство назначенной третьей стороны, сопряженное с устройством приема.

Если указанные наборы идентификационных данных, связанных с предъявителем, находятся в указанных записях на указанном управляющем сервере, выполненном с возможностью обеспечения извлечения и выдачи контролируемых идентификационных данных, этапы извлечения связанного с предъявителем набора идентификационных данных и передачи связанного с предъявителем набора идентификационных данных могут быть выполнены на указанном управляющем сервере, выполненном с возможностью обеспечения извлечения и выдачи контролируемых идентификационных данных.

Если указанные наборы идентификационных данных, связанных с предъявителем, находятся в отдельных отметках на другом сервере, отличном от указанного управляющего сервера, выполненном с возможностью обеспечения извлечения и выдачи контролируемых идентификационных данных, (этап идентификации отметки, относящейся к связанному с предъявителем набору идентификационных данных, может быть выполнен на указанном другом сервере, отличном от указанного управляющего сервера, выполненном с возможностью обеспечения извлечения и выдачи контролируемых идентификационных данных), причем этапы извлечения связанного набора идентификационных данных и выдачи связанного набора идентификационных данных могут быть выполнены либо на управляющем сервере, выполненном с возможностью обеспечения извлечения и выдачи набора идентификационных данных, связанных с предъявителем, либо на другом сервере, отличном от управляющего сервера, выполненном с возможностью обеспечения извлечения и выдачи набора идентификационных данных, связанных с предъявителем.

Этап поиска соответствия между общими ключами может дополнительно включать установление того, истек ли период достоверности.

Этап поиска соответствия между общими ключами может дополнительно включать поиск соответствия между предварительно определенным вспомогательным параметром, содержащимся в сообщении устройства приема, и соответствующим предварительно определенным вспомогательным параметром, содержащимся в сообщении устройства предъявления.

Если период достоверности назначен одноразовому общему ключу, указанный общий ключ может быть уникальным в течение длительности его периода достоверности.

В другом аспекте настоящего изобретения способ включает (a) предоставление доступа устройством приема к одноразовому общему ключу для предъявляющей стороны взаимодействия; (b) получение секретного ключа предъявителя, принадлежащего предъявляющей стороне взаимодействия, на устройстве приема, причем указанный секретный ключ предъявителя вводит на терминале предъявляющая сторона взаимодействия; (c) передачу сообщения устройства приема от устройства приема на сервер, причем сообщение устройства приема содержит одноразовый общий ключ и секретный ключ предъявителя; (d) получение устройством предъявления одноразового общего ключа; (e) извлечение устройством предъявления идентификатора предъявителя, принадлежащего предъявляющей стороне взаимодействия, из места хранения на устройстве предъявления; и (f) передачу устройством предъявления сообщения устройства предъявления на управляющий сервер, причем сообщение устройства предъявления содержит одноразовый общий ключ и идентификатор предъявителя.

Целевая запись на указанном сервере также может дополнительно содержать условное название, соответствующее указанной отметке, относящейся к каждому набору идентификационных данных, связанных с предъявителем, и сообщение устройства предъявления может дополнительно содержать копию условного названия, выбранную из списка условных названий, составленного на устройстве предъявления, и причем на этапе выполнения поиска целевой записи, которая содержит такой же идентификатор предъявителя и секретный ключ, также используют условное название, содержащееся в сообщении уст-

ройства предъявления, для поиска целевой записи, содержащей такое же указанное условное название в дополнение к такому же идентификатору предъявителя и секретному ключу.

Набор идентификационных данных может находиться в виде отметки в указанной целевой записи на указанном управляющем сервере, выполненном с возможностью обеспечения извлечения и выдачи контролируемых идентификационных данных, и этапы извлечения набора идентификационных данных и выдачи набора идентификационных данных выполняют на указанном управляющем сервере, выполненном с возможностью обеспечения извлечения и выдачи контролируемых идентификационных данных.

Набор идентификационных данных может находиться в виде отметки на другом сервере, отличном от указанного управляющего сервера, выполненном с возможностью обеспечения извлечения и выдачи контролируемых идентификационных данных, причем отдельная отметка связана с целевой записью, и причем этапы извлечения и выдачи набора идентификационных данных могут быть выполнены либо на указанном управляющем сервере, выполненном с возможностью обеспечения извлечения и выдачи контролируемых идентификационных данных, либо на другом сервере, отличном от управляющего сервера, выполненном с возможностью обеспечения извлечения и выдачи контролируемых идентификационных данных.

Дополнительный аспект настоящего изобретения относится к устройству предъявления, выполненному с возможностью выполнения одного или более описанных выше этапов, связанных с устройством предъявления.

Другой аспект настоящего изобретения относится к устройству приема, выполненному с возможностью выполнения одного или более описанных выше этапов, связанных с устройством приема.

Дополнительный аспект настоящего изобретения относится к серверу, выполненному с возможностью выполнения одного или более описанных выше этапов, связанных с указанным сервером.

Еще один аспект настоящего изобретения относится к системе, содержащей два или более устройства предъявления, два или более устройства приема и указанный управляющий сервер, выполненный с возможностью выполнения одного или более описанных выше вариантов осуществления.

Дополнительный аспект настоящего изобретения относится к машиночитаемому носителю данных, на котором хранится компьютерная программа, причем указанная программа содержит машинные команды, приспособленные для выполнения одного или более описанных выше этапов способа при исполнении одним или более модулями обработки.

Подробное описание

На фиг. 1 представлена схема, изображающая центральную систему для сохранения секретности таким образом, который также способствует разрешенной выдаче хранящегося набора идентификационных данных получателю, утвержденному участником, к которому относится набор идентификационных данных. Система 100 является надежной в том, что она защищает наборы идентификационных данных от несанкционированного доступа со стороны неуполномоченных потенциальных получателей наборов идентификационных данных, а также предотвращает наборы идентификационных данных от использования теми, кто в результате мошенничества предъявляет набор идентификационных данных как свой собственный. Стороны, зарегистрированные с помощью системы, обозначаются как "предъявители" и "приемщики" в соответствии с их ролью в способе согласно настоящему изобретению и характером их взаимодействия с системой согласно настоящему изобретению. В ходе взаимодействия между предъявителем и приемщиком предъявителю может быть необходимо выдать набор идентификационных данных, который ему соответствует. Предъявители и приемщики, активно участвующие в таком взаимодействии, соответственно обозначаются как "предъявляющие стороны взаимодействия" и "принимающие стороны взаимодействия". Следует понимать, что во многих вариантах осуществления настоящего изобретения каждому из предъявителей соответствуют наборы идентификационных данных, которые являются уникальными для них, так что предъявители связаны с наборами идентификационных данных "взаимно-однозначным" образом. Однако настоящее изобретение также предусматривает варианты с взаимоотношением типа "множество-один" между предъявителями и наборами идентификационных данных, причем множеству предъявителей соответствует один набор идентификационных данных, и по-прежнему предпочтительно поддерживать указанный набор идентификационных данных в состоянии секретности.

В соответствии с одним вариантом осуществления настоящего изобретения система и способ согласно настоящему изобретению используются такой предъявляющей стороной взаимодействия для выдачи набора идентификационных данных, соответствующих указанной предъявляющей стороне взаимодействия, одному или более назначенным получателям таким образом, который поддерживает секретность набора идентификационных данных. В соответствии с другими вариантами осуществления настоящего изобретения система и способ согласно настоящему изобретению могут быть использованы принимающей стороной взаимодействия для выдачи набора идентификационных данных, соответствующих принимающей стороне взаимодействия, одному или более назначенным получателям, при этом сохраняя указанное состояние секретности. Другие варианты осуществления настоящего изобретения предусматривают одновременное предоставление наборов идентификационных данных как предъявителя, так приемщика, связанных соответственно с предъявляющей стороной взаимодействия и принимающей стороной взаимодействия. И предъявитель, и приемщик сотрудничают, чтобы способствовать выда-

че таких наборов идентификационных данных из системы. Назначенный получатель может быть принимающей стороной взаимодействия, предъявляющей стороной взаимодействия или может быть доверенной третьей стороной.

Система 100 содержит по меньшей мере один сервер 101, причем сервер содержит группу записей 102 предъявителя. Каждая запись предъявителя относится к данному участнику, который зарегистрирован как предъявитель указанным сервером 101, и каждая указанная запись содержит один или более наборов идентификационных данных, относящихся к этому предъявителю. Более конкретно, каждая запись предъявителя содержит идентификатор предъявителя, секретный ключ предъявителя, по меньшей мере один набор идентификационных данных, соответствующий указанному предъявителю, и по меньшей мере одно условное название, причем каждый набор идентификационных данных связан соответственно с одним условным названием, вследствие чего каждое условное название в записи предъявителя можно отличить от оставшихся условных названий в указанной записи предъявителя. Идентификатор предъявителя представляет собой уникальную строку символов, используемую для идентификации данной записи предъявителя в группе записей предъявителя. Секретный ключ предъявителя представляет собой строку символов, известную только предъявителю. Когда предъявитель взаимодействует с системой с целью выдачи набора идентификационных данных предъявителя, назначенному получателю (такой предъявитель называется как "предъявляющая сторона взаимодействия"), он предъявляет свой идентификатор предъявителя, причем его секретный ключ предъявителя затем может использоваться для установления подлинности предъявляющей стороны взаимодействия перед выдачей каких-либо наборов идентификационных данных. В дополнение к идентификатору предъявителя и секретному ключу предъявителя каждая запись предъявителя содержит по меньшей мере один набор идентификационных данных. Как было описано ранее, каждый набор идентификационных данных содержит набор личных данных, характерных для лица и необходимых для указанного взаимодействия. Каждому набору идентификационных данных также соответствует отличимое условное название. В целях пояснения лицо по имени "Джон Браун" может иметь первый набор идентификационных данных, относящийся к водительскому удостоверению, и второй набор идентификационных данных, относящийся к карте постоянного покупателя магазина. Первый набор идентификационных данных может содержать имя "Джон Браун", дату рождения, номер водительского удостоверения и дату окончания его действия. Второй набор идентификационных данных может содержать имя "Джон Браун", адрес и членский номер клуба. Первому набору идентификационных данных может соответствовать условное название "водительское удостоверение", при этом второму набору идентификационных данных может соответствовать условное название "клубная карта 1". Следует понимать, что в вариантах осуществления настоящего изобретения, в которых предусматривается, что каждая запись предъявителя будет содержать только один набор идентификационных данных, может не требоваться, чтобы записи предъявителя дополнительно содержали условное название, связанное с каждым набором идентификационных данных. То есть, в таких случаях, идентификация записи, относящейся к взаимодействующему предъявителю, автоматически будет также указывать набор идентификационных данных, подлежащих выдаче.

Кроме того, в некоторых вариантах осуществления настоящего изобретения сервер 101 также содержит группу отдельных записей приемщика. Каждая запись приемщика относится к лицу или организации, зарегистрированной в качестве приемщика сервером, и содержит один или более наборов идентификационных данных, соответствующих этому приемщику. Каждая запись приемщика дополнительно содержит идентификатор приемщика и необязательно секретный ключ приемщика. Идентификатор приемщика представляет собой уникальную строку символов, используемую для идентификации данной записи приемщика в группе записей приемщика. Секретный ключ приемщика (если он имеется) представляет собой строку символов, известную только приемщику. Когда приемщик взаимодействует с системой, для того чтобы способствовать выдаче набора идентификационных данных предъявителя, соответствующего предъявляющей стороне взаимодействия, назначенному получателю (такой приемщик называется как "принимающая сторона взаимодействия"), предъявляется идентификатор приемщика принимающей стороны взаимодействия, и секретный ключ приемщика принимающей стороны взаимодействия (если он используется) может затем применяться для установления подлинности принимающей стороны взаимодействия перед выдачей каких-либо наборов идентификационных данных.

Следует понимать, что хотя в описанном варианте осуществления настоящего изобретения записи предъявителя и записи приемщика отличаются и, как правило, хранятся в виде отдельных групп записей, в других вариантах осуществления настоящего изобретения сервер 101 может содержать одну группу записей, содержащую записи как предъявителя, так и приемщика. Кроме того, также следует понимать, что хотя в одном варианте осуществления наборы идентификационных данных приемщика и/или предъявителя хранятся на одном сервере, также предусматривается возможность использования нескольких серверов, причем задачей каждого сервера является хранение записей, содержащих один или более типов наборов идентификационных данных.

Дополнительно предусматривается, что в некоторых вариантах осуществления настоящего изобретения сервер 101 будет содержать исключительно записи предъявителя и не будет содержать записи приемщика. Предпочтительно в таких вариантах осуществления сервер 101 и потенциальные принимающие

стороны взаимодействия смогут обмениваться данными друг с другом с помощью своих существующих систем программного обеспечения. Этот вариант осуществления настоящего изобретения является предпочтительным, поскольку предварительная регистрация приемщиков не требуется, что устраняет препятствия, мешающие внедрению заявляемых системы и способа среди потенциальных принимающих сторон взаимодействия. Таким образом, это упрощает использование системы и способа.

Сервер 101 может обмениваться данными с одним или более устройствами 109 по каналу связи. Следует понимать, что канал 107 связи может включать сеть Интернет, фирменную сеть или их комбинацию. Устройство 109 может быть расположено отдельно и может быть соединено с каналом 107 связи посредством одного или более из ряда технологий, таких как PSTN, Ethernet, DSL, ISDN, Wi-Fi, WiMax, 2G, 3G, LTE, 4G и т.д. Устройства 109 могут представлять собой любое из ряда приборов, включающих настольные персональные компьютеры, портативные компьютеры, планшетные персональные компьютеры, карманные персональные компьютеры, мобильные телефоны, смартфоны и т.д. В альтернативном варианте устройство 109 может содержать вычислительные системы, сделанные под заказ, которые используются в ряде отраслей, включая банковское дело, финансовую сферу, авиацию, туризм, сферу государственной безопасности, пограничный контроль, энергетику, транспорт, розничную продажу и/или телекоммуникации. Соответственно устройства могут содержать приборы, выполненные с возможностью работы в качестве приборов для точек продажи. В контексте настоящего изобретения эти устройства будут называться как "устройства приема".

Сервер 101 также может обмениваться данными по каналу 106 связи с одним или более устройствами 108. Такие устройства могут содержать, например, беспроводные приборы, которые могут обмениваться данными с сервером 101 посредством беспроводной базовой станции или маршрутизатора. Беспроводные приборы могут включать беспроводной прибор любого типа, включая портативные компьютеры, планшетные персональные компьютеры, карманные персональные компьютеры, мобильные телефоны, смартфоны и т.д. Такие периферийные приборы могут дополнительно включать приборы, выполненные с возможностью обмена данными по каналу 106 связи посредством проводного соединения, и могут, таким образом, например, содержать настольные компьютеры, а также вышеупомянутые характерные для отрасли вычислительные системы, сделанные под заказ, включая без ограничения системы точки продажи. В контексте настоящего изобретения эти периферийные приборы будут называться как "устройства предъявления". В одном варианте осуществления устройство предъявления также может быть защищено паролем или может потребовать дополнительно разрешение от предъявителя для инициации связи. Периферийные устройства предъявления могут быть расположены отдельно и могут обмениваться данными с сервером 101 по каналу 108 связи с помощью ряда средств, таких как PSTN, Ethernet, DSL и ISDN. Устройства предъявления, содержащие беспроводные приборы, могут обмениваться данными с сервером 101 посредством одного или более из ряда технологий беспроводной связи, таких как Wi-Fi, WiMax, 2G, 3G, LTE, 4G и т.д. Канал 106 связи может содержать сеть Интернет, фирменную сеть или их комбинацию. Устройства 108 предъявления выполнены с приложением, которое способно установить связь с сервером 101. Поскольку соединение между устройствами 109 приема и сервером 101 содержит первый канал 107 связи и соединение между устройствами 108 предъявления и сервером 101 содержит второй канал 106 связи, систему 100 можно рассматривать как "многоканальную" по ее составу. Это обеспечивает более надежный механизм, с помощью которого наборы идентификационных данных и другие конфиденциальные данные могут храниться и быть выданы на конечную точку 110 сети, при этом сохраняя состояние секретности. Конечная точка 110 сети в некоторых вариантах осуществления может представлять собой или отдельное устройство, или само устройство приема в зависимости от указанного пункта назначения в сообщении устройства приема.

Хотя в этом варианте осуществления было описано, что наборы идентификационных данных и связанные с ними условные названия находятся в записях предъявителя и/или приемщика на сервере, в других вариантах осуществления настоящего изобретения предполагается, что указанные наборы идентификационных данных и связанные с ними условные названия могут быть связаны с указанными записями предъявителя и/или приемщика альтернативными путями. Например, наборы идентификационных данных и связанные с ними условные названия могут находиться в одном или более наборах записей, отличных от набора (наборов) записей на сервере, содержащего записи, содержащие идентификаторы и секретные ключи. Эти отдельные наборы записей могут храниться на одном или более отличных серверах. В некоторых вариантах осуществления настоящего изобретения отличные серверы, хранящие наборы идентификационных данных, находятся под управлением контроллеров, отвечающих за выдачу документов, содержащих указанные наборы идентификационных данных.

На фиг. 2 представлена блок-схема, на которой изображен принцип, по которому новый потенциальный пользователь регистрируется с помощью сервера 101 в качестве предъявителя в соответствии с одним вариантом осуществления настоящего изобретения. На этапе 200 новый пользователь-предъявитель получает доступ к веб-странице, размещенной на сервере 101, предпочтительно с помощью своих устройств 108 предъявления. Веб-страница выполнена таким образом, что на этом этапе новый пользователь-предъявитель предоставляет общие сведения для регистрации, такие как имя, адрес, адрес электронной почты, страну проживания и т.д., и отправляет их на сервер 101. Следует понимать,

что хотя в некоторых вариантах осуществления настоящего изобретения сведения для регистрации предоставляются непосредственно на сервер 101, в других вариантах осуществления сведения для регистрации могут быть предоставлены предварительно косвенным путем для предварительной обработки перед вводом сведений на сервер 101. Доступ к веб-странице может быть получен по соединению в течение длительности процедуры, или же могут использоваться исключительно безопасные соединения только в случае передачи конфиденциальной информации (такой как набор идентификационных данных или дополнительные данные, такие как секретный ключ предъявителя). Также следует понимать, что возможны альтернативные средства регистрации, например отправка заполненной формы по почте, факсу и т.д.

Затем на этапе 202 на сервере 101 создается новая учетная запись для пользователя-предъявителя. Это осуществляется путем генерирования новой записи предъявителя в группе записей предъявителя. На этапе 200 или на этапе 202 новому пользователю-предъявителю предлагается выбрать и ввести новый секретный ключ предъявителя, который затем добавляется в новую запись предъявителя пользователя-предъявителя. В альтернативных вариантах осуществления настоящего изобретения новая запись предъявителя может быть автоматически снабжена временным секретным ключом предъявителя, который может быть впоследствии заменен секретным ключом предъявителя, самостоятельно выбранным пользователем-предъявителем в дальнейшем. Такой временный секретный ключ может быть предоставлен с помощью веб-страницы или предпочтительно с помощью второго канала связи, который может содержать сообщение любого типа, включая электронное сообщение, сообщение SMS, телефонный звонок или сообщение, отправленное по почте. В некоторых вариантах осуществления настоящего изобретения существует дополнительная возможность для предоставления заменяющего секретного ключа, например, на случай, если первоначальный секретный ключ забыт или вызывает сомнение. Такие заменяющие секретные ключи могут быть аналогичным образом предоставлены посредством сообщения любого вида, включая посредством сайта, электронного сообщения, SMS, телефонного звонка или сообщения, отправленного по почте.

На этапе 204 новому пользователю-предъявителю предлагается добавить наборы идентификационных данных в только что созданную учетную запись нового пользователя-предъявителя. Как было описано ранее, эти наборы идентификационных данных могут содержать ряд личных данных и могут относиться к документам, содержащим набор идентификационных данных, выданным рядом различных государственных или коммерческих органов надзора. Каждый набор идентификационных данных будет связан с условным названием, которое является уникальным для его родительской записи предъявителя (т.е. каждое условное название является "локально уникальным"). В одном варианте осуществления на этапе 206 новому пользователю-предъявителю может быть предложено предоставить локально уникальное условное название для каждого предоставленного набора идентификационных данных. В другом варианте осуществления для каждого набора идентификационных данных может быть предоставлено заданное по умолчанию условное название. В одном варианте осуществления условные названия могут быть впоследствии отредактированы предъявителем. В некоторых вариантах осуществления настоящего изобретения запись предъявителя может быть отредактирована после регистрации следующим образом: существующие наборы идентификационных данных и связанные с ними условные названия могут быть отредактированы или удалены и/или новые наборы идентификационных данных и связанные с ними условные названия могут быть добавлены. В некоторых вариантах осуществления настоящего изобретения запись предъявляющей стороны взаимодействия может быть отредактирована после регистрации следующим образом: существующие наборы идентификационных данных и связанные с ними условные названия могут быть отредактированы или удалены и новые наборы идентификационных данных и связанные с ними условные названия могут быть добавлены.

На этапе 206 новому пользователю-предъявителю предоставляется возможность задать характерные предпочтения, связанные с обработкой и использованием наборов идентификационных данных, соответствующие конкретным государственным или коммерческим органам надзора, и типы взаимодействия, к которым они относятся. В качестве примера касательно набора идентификационных данных, относящегося к участию программы лояльности авиакомпании, предъявителю может быть предоставлено право задать дополнительные предпочтения в соответствии с его предпочтениями членства, например предпочтительное бортовое питание, предпочтительное место или местный аэропорт. В качестве другого примера касательно набора идентификационных данных, относящегося к кредитной карте, предъявителю может быть предоставлено право подключить функциональные возможности, такие как предпочтительное использование карты, прямая конвертация валют, налог на добавленную стоимость, возврат денег путешественникам или дробная оплата по нескольким картам.

На этапе 208 новому пользователю-предъявителю затем предлагается установить специальное приложение на его устройство 108 предъявления. Специальное приложение выполнено с возможностью способствовать установлению связи с сервером по мере необходимости во время процесса разрешения выдачи сервером набора идентификационных данных и процесса установления подлинности такого переданного разрешения, как будет подробно описано ниже. В течение хода установки специального приложения приложению соответствует уникальный идентификатор предъявителя, который хранится на устройстве предъявления. В предпочтительном варианте осуществления идентификатор предъявителя при-

сваивается сервером и встраивается в приложение перед, во время или после установки приложения на устройство предъявления. Альтернативно, идентификатор предъявителя может быть получен из последовательности символов, свойственной устройству предъявления, например номер IMEI или серийный номер. Эта последовательность символов может быть модифицирована для получения уникального идентификатора предъявителя. В дополнение к хранению на устройстве предъявления идентификатор предъявителя также добавляется в запись предъявителя в группе записей предъявителя на сервере 101. В течение хода установки специального приложения приложение также получает условные названия, связанные с наборами идентификационных данных, сохраненными на этапе 204 для данного предъявителя. Соответственно, когда приложение используется при взаимодействии новым предъявителем, оно распознает как идентификатор предъявителя, так и условные названия, связанные с наборами идентификационных данных нового предъявителя, таким образом, что идентификатор предъявителя и условное название могут быть переданы на сервер 101 соответственно.

В предпочтительном варианте осуществления на устройство предъявления нового пользователя-предъявителя вначале может быть установлена стандартная версия приложения. По окончании процесса, изображенного на этапах 200-208, новому пользователю-предъявителю может быть предложено подтвердить подлинность своей учетной записи путем ответа на электронное сообщение и/или путем подтверждения своего секретного ключа предъявителя в ответ на запрос от сервера. По окончании указанного подтверждения подлинности стандартная версия приложения на устройстве предъявления нового пользователя-предъявителя может быть настроена с идентификатором предъявителя нового пользователя-предъявителя, условными названиями, связанными с наборами идентификационных данных нового пользователя-предъявителя и предпочтениями нового пользователя-предъявителя, выбранными на этапе 206. Эти данные могут храниться в зашифрованном формате на устройстве предъявления нового пользователя-предъявителя. На фиг. 3 представлена блок-схема, аналогичная блок-схеме на фиг. 2, изображающая этапы, с помощью которых сторона может зарегистрироваться в качестве приемщика с помощью сервера 101 в соответствии с одним вариантом осуществления настоящего изобретения. Как было указано ранее, настоящее изобретение предусматривает варианты осуществления, в которых приемщик должен активно регистрироваться с помощью сервера, а также варианты осуществления, в которых приемщик не должен регистрироваться с помощью сервера. Кроме того, в других вариантах осуществления настоящего изобретения регистрация приемщика может быть выполнена "пассивно", как будет описано более подробно ниже. На этапе 300 к веб-странице, размещенной на сервере 101, получает доступ сторона (здесь и далее называемая как "новый пользователь-приемщик"), предпочтительно с помощью устройства 109 приема. Аналогично этапу 200 на фиг. 2 веб-страница выполнена таким образом, что на этом этапе новый пользователь-приемщик предоставляет общие сведения для регистрации, такие как имя лица или название организации, адрес, адрес электронной почты и т.д., и отправляет их на сервер 101. Доступ к веб-странице может быть получен по безопасному соединению в течение длительности процедуры, или же могут использоваться исключительно безопасные соединения только в случае передачи конфиденциальной информации (такой как секретный ключ приемщика или набор идентификационных данных приемщика). Также следует понимать, что регистрация нового пользователя-приемщика может быть выполнена с помощью других средств, таких как почта или факс. Альтернативно, если приемщик использует устройство приема, которое находится под удаленным управлением соответствующей третьей стороны (такой как, например, терминальные системы управления, используемые эквайерами для управления приборами для точек продажи с карточными платежами), регистрация приемщика может быть инициирована соответствующей третьей стороной. В таких вариантах приемщику может не потребоваться самому предоставлять какую-либо информацию.

На этапе 302 новая учетная запись создается на сервере 101 путем генерирования записи нового пользователя-приемщика в группе записей приемщика.

Для обеспечения возможности предоставления набора идентификационных данных предъявителя должно быть выдано разрешение, как описано ниже. В одном варианте осуществления настоящего изобретения при предоставлении любого разрешения, исходящего от приемщика, на выдачу набора идентификационных данных предъявителя будет необходимо, чтобы приемщик был идентифицирован, и, следовательно, при предоставлении любого разрешения на выдачу набора идентификационных данных предъявителя вначале может потребоваться предоставление набора идентификационных данных приемщика. Соответственно предусматривается, что как и для записей предъявителя, в записи приемщика требуется отдельный набор идентификационных данных приемщика для каждого типа взаимодействия, в котором приемщик желает принять участие. Типы взаимодействия могут быть определены в широком смысле, например, выдача документа в виде водительского удостоверения и выдача документа в виде платежной карты могут расцениваться как различные типы взаимодействия. Альтернативно, типы взаимодействия могут быть определены в узком смысле, например, выдача различных документов в виде платежной карты (например, Mastercard, Visa Debit) может расцениваться как различные типы взаимодействия. Соответственно хотя в некоторых вариантах осуществления, например, набор идентификационных данных приемщика может, в целом, применяться ко всем платежным картам, в других вариантах осуществления приемщик может иметь разные наборы идентификационных данных для каждого отлич-

ного типа платежной карты, обрабатываемой приемщиком.

На этапе 306 новому пользователю-приемщику предоставляется возможность задать характерные предпочтения, связанные с обработкой и использованием наборов идентификационных данных, соответствующих конкретным типам взаимодействия. В качестве примера касательно набора идентификационных данных, относящегося к кредитной карте, новому пользователю-приемщику может быть предоставлено право указать свое желание по предоставлению нисходящих функциональных возможностей, соответствующих набору идентификационных данных, после выдачи набора идентификационных данных приемщика, например прямая конвертация валют, налог на добавленную стоимость, возврат денег путешественникам или дробная оплата по нескольким картам.

Затем на этапе 308 устройство приема выполнено таким образом, что оно может обмениваться данными с сервером. Это может быть осуществлено рядом способов. В тех вариантах осуществления настоящего изобретения, в которых устройство приема находится под удаленным управлением третьей стороны, третья сторона может инициировать автоматическую перенастройку устройства приема, если это необходимо. В других вариантах осуществления настоящего изобретения новый пользователь-приемщик может инициировать перенастройку путем установки специального приложения аналогично описанному на фиг. 2.

На фиг. 4 представлена блок-схема, изображающая способ обеспечения выдачи по меньшей мере одного набора контролируемых идентификационных данных, связанных с предъявителем, при этом поддерживая секретность, имеющую приоритетное значение в указанных идентификационных данных, в соответствии с одним вариантом осуществления настоящего изобретения. Управляющий сервер получает сообщение устройства приема, содержащее секретный ключ и одноразовый общий ключ, и сообщение устройства предъявления, содержащее идентификатор предъявителя и одноразовый общий ключ. На этапе 403 информационные сообщения сравнивают. В случае отсутствия соответствия способ прекращают и команду взаимодействия не выполняют. В случае соответствия общих ключей на этапе 404 иницируют поиск целевой записи на сервере путем связывания секретного ключа и идентификатора предъявителя. Выполняют поиск любой целевой записи, содержащей такие же идентификатор предъявителя и секретный ключ, что и содержащиеся в сообщении устройства приема и сообщении устройства предъявления. В случае нахождения целевой записи набор идентификационных данных, относящийся к месту хранения, присутствующему в записи, извлекают и разрешают его выдачу в указанный пункт назначения, который представляет собой конечную точку сети.

На фиг. 5А и 5В изображен процесс, выполняемый в устройстве приема. Устройство приема генерирует одноразовый общий ключ и передает его на устройство предъявления. Устройство приема также принимает секретный ключ предъявителя и генерирует сообщение, которое должно быть отправлено на управляющий сервер, как показано позицией 101 на фиг. 1. Указанное сообщение содержит секретный ключ предъявителя и одноразовый общий ключ.

На фиг. 6А и 6В изображен процесс, выполняемый в устройстве предъявления. Идентификатор предъявителя извлекают из запоминающего устройства. После получения одноразового общего ключа от устройства приема сообщение, содержащее идентификатор предъявителя и одноразовый общий ключ, передают на управляющий сервер 101. На фиг. 7 и 8 представлены отметки, относящиеся к контролируемым идентификационным данным, связанным с предъявителем. Каждой из отметок соответствует идентификатор предъявителя и секретный ключ. На фиг. 7А-7Е представлены различные варианты осуществления хранения записей на управляющем сервере или сервере 101 с идентификационными данными. В некоторых вариантах осуществления записи предъявляющей стороны взаимодействия могут быть замаскированы и размещены с использованием таблиц поиска, изображенных на фиг. 7А и 7С. Возможен другой вариант осуществления, в котором каждой записи стороны взаимодействия-предъявителя соответствует условное название.

На фиг. 9А и 9В показаны графические представления, относящиеся к процессу передачи сообщений на управляющем сервере от предъявляющей и принимающей сторон взаимодействия и процессу отправки контролируемых идентификационных данных в разрешенные пункты назначения. На фиг. 10 представлена диаграмма последовательности действий, изображающая процесс, посредством которого может быть предоставлено разрешение в соответствии с одним вариантом осуществления настоящего изобретения, включающий сервер 1001, предъявляющую сторону 1002 взаимодействия, устройство 1003 предъявления, конечную точку 1004 сети и устройство 1005 приема, который предназначен для извлечения набора идентификационных данных из места хранения, идентифицированного предъявляющей стороной 1002 взаимодействия, и выдачи набора идентификационных данных на оборудование получателя, разрешенное предъявляющей стороной 1002 взаимодействия. Следует понимать, что предоставление разрешения на извлечение и выдачу набора идентификационных данных предъявителя также может одновременно сопровождаться запросом на извлечение набора идентификационных данных приемщика, причем устройство 1005 приема и устройство 1003 предъявления по-прежнему отправляют свои соответствующие сообщения на сервер 1001. Также следует понимать, что в некоторых вариантах осуществления настоящего изобретения разрешение на выдачу набора идентификационных данных в конкретном случае будет представлять собой разрешение на выдачу набора идентификационных данных предъявите-

ля (соответствующего предъявляющей стороне 1002 взаимодействия) на конечную точку 1004 сети или устройство 1005 приема. Однако в других вариантах осуществления настоящего изобретения будет предоставлено разрешение на совместное использование набора идентификационных данных приемщика или предъявителя доверенной третьей стороне, соответствующей конечной точке 1004 сети или устройству 1005 приема. Например, если отправлено разрешение на совместное использование набора идентификационных данных предъявителя, относящегося к документу в виде платежной карты, возможно, оно может быть предназначено для отправки набора идентификационных данных платежной карты на процессор транзакций доверенной третьей стороны.

На фиг. 10 предъявляющая сторона 1002 взаимодействия, обладающая устройством 1003 предъявления, выполненным с возможностью генерирования и передачи сообщения устройства предъявления на сервер 1001, идентифицирует оборудование, работающее на принимающей стороне взаимодействия, которое содержит конечную точку 1004 сети и/или устройство 1005 приема (причем конечная точка 1004 сети представляет собой устройство 1005 приема или причем конечная точка 1004 сети связана с устройством 1005 приема), и при этом устройство 1005 приема выполнено с возможностью генерирования и передачи сообщения устройства приема на сервер 1001. Предъявляющая сторона 1002 взаимодействия может решить взаимодействовать с таким оборудованием с целью разрешения чтения набора идентификационных данных, связанного с предъявляющей стороной 1002 взаимодействия, который должен быть выдан на конечную точку 1004 сети или устройство 1005 приема. Принимающая сторона взаимодействия также может решить взаимодействовать с таким оборудованием с целью отправки запроса на чтение набора идентификационных данных, связанного с принимающей стороной взаимодействия, который должен быть возвращен на конечную точку 1004 сети или устройство 1005 приема при получении набора идентификационных данных, связанного с предъявляющей стороной 1002 взаимодействия, на конечной точке 1004 сети или устройстве 1005 приема. Более конкретно, в предпочтительном варианте осуществления настоящего изобретения сохраняется состояние секретности, имеющее приоритетное значение в идентификационных данных, связанных с предъявляющей стороной 1002 взаимодействия, при этом чтение набора идентификационных данных, связанных с предъявляющей стороной 1002 взаимодействия, не является видимым или доступным для принимающей стороны взаимодействия и не передается на устройство 1003 предъявления или с помощью него, а передается только конфиденциально на конечную точку 1004 сети или устройство 1005 приема.

На фиг. 10 во время происходящего события 1010 сигнал передают с конечной точки 1004 сети или устройства 1005 приема на предъявляющую сторону 1002 взаимодействия, что обозначает, что указанный способ, предложенный в настоящем изобретении, является способом, доступным на конечной точке 1004 сети или устройстве 1005 приема для предъявляющей стороны 1002 взаимодействия, при этом конечная точка 1004 сети снабжена таким устройством 1005 приема, и причем такое устройство 1005 приема выполнено с возможностью обмена данными с сервером 1001. Фактически, указанный способ, предложенный в настоящем изобретении, представляет собой один из способов, доступных на конечной точке 1004 сети для получения идентификационных данных от предъявляющей стороны 1002 взаимодействия.

На фиг. 10 во время происходящего события 1011 предъявляющая сторона 1002 взаимодействия решает инициировать взаимодействие на оборудовании, работающем на принимающей стороне взаимодействия, согласно ходу выполнения способа, предложенного в настоящем изобретении, путем использования устройства 1003 предъявления, выполненного с возможностью генерирования и передачи сообщения устройства предъявления на такой сервер 1001, и использования устройства 1005 приема, выполненного с возможностью генерирования и передачи сообщения устройства приема на сервер 1001. Фактически, предъявляющая сторона 1002 взаимодействия делает выбор инициировать взаимодействие на оборудовании принимающей стороны взаимодействия согласно ходу выполнения способа, предложенного в настоящем изобретении, отказываясь от инициации взаимодействия на оборудовании, работающем на принимающей стороне взаимодействия, согласно любому другому ходу выполнения способов, доступных на конечной точке 1004 сети для получения идентификационных данных от предъявляющей стороны 1002 взаимодействия.

На стадии 1012 взаимодействие инициируют путем активации устройства 1005 приема, которое выполнено с возможностью способствовать установлению устройством приема связи с сервером 1001. После активации на стадии 1012 одноразовый общий ключ создают 1012 на устройстве 1005 приема. В одном варианте осуществления сервер 1001 генерирует общий ключ и передает на устройство 1005 приема. В другом варианте осуществления общий ключ генерируют на устройстве 1005 приема.

На стадии 1013 взаимодействие инициируют путем активации устройства 1003 предъявления, способствующего установлению связи устройства предъявления с сервером 1001. После активации на стадии 1013 идентификатор предъявителя извлекают из места хранения на устройстве 1003 предъявления. В одном варианте осуществления список условных названий, соответствующих идентификационным данным, связанным с предъявляющей стороной 1002 взаимодействия, относящийся к идентификатору предъявителя, также извлекают из определенного места хранения на устройстве 1003 предъявления. В таком варианте осуществления такой список условных названий, соответствующий идентификационным

данным, связанным с предъявляющей стороной взаимодействия, составляют на устройстве 1003 предъявления для выбора предъявляющей стороной 1002 взаимодействия.

На стадии 1014 к общему ключу предоставляют доступ на устройстве 1005 приема для предъявляющей стороны 1002 взаимодействия и устройства 1003 предъявления. В одном варианте осуществления стадии 1014 его делают человекочитаемым на устройстве 1005 приема. В другом варианте осуществления стадии 1014 его делают машиночитаемым на устройстве 1005 приема.

На стадии 1015 общий ключ получают соответственно на устройстве 1003 предъявления. В одном варианте осуществления его получают путем его чтения на устройстве 1005 приема и ввода его в устройство 1003 предъявления. В другом варианте осуществления его получают путем сканирования его на устройстве 1005 приема и захвата его на устройстве 1003 предъявления. В одном варианте осуществления устройство 1005 приема передает одноразовый общий ключ непосредственно 1014 на устройство 1003 предъявления, при этом в другом варианте осуществления устройство 1005 приема предоставляет доступ к общему ключу 1014 для предъявляющей стороны 1002 взаимодействия, которая вводит его на стадии 1016 в устройство 1003 предъявления. В некоторых вариантах осуществления настоящего изобретения общему ключу может быть назначен период достоверности. Это гарантирует то, что если принятое сообщение устройства приема и принятое сообщение устройства предъявления не соответствуют друг другу в течение определенного интервала времени путем поиска соответствия между одноразовыми общими ключами (как описано ниже) в течение определенного интервала времени (периода достоверности), то взаимодействие может прекратиться и, таким образом, завершиться, делая дальнейшие процессы лишними. После истечения периода достоверности общего ключа тот же общий ключ, таким образом, может быть повторно использован в последующей итерации способа. Соответственно период достоверности может обеспечить возможность использования более коротких и менее сложных секретных ключей, поскольку таким образом становится целесообразным повторное использование общего ключа. Это является предпочтительным в вариантах осуществления настоящего изобретения, в которых предъявляющей стороне взаимодействия необходимо ввести общий ключ в устройство 1003 предъявления, поскольку сниженная сложность ключа делает более удобным этот вариант осуществления способа.

В некоторых вариантах осуществления устройство 1003 предъявления также может отображать список условных названий, относящихся к различным наборам идентификационных данных предъявителя, связанным с указанной предъявляющей стороной 1002 взаимодействия. Затем предъявляющая сторона 1002 взаимодействия выбирает условное название, соответствующее требуемому набору идентификационных данных, связанному с предъявляющей стороной 1002 взаимодействия.

На стадии 1016 устройство приема пытается получить секретный ключ предъявляющей стороны 1002 взаимодействия путем выдачи инструкций предъявляющей стороне 1002 взаимодействия ввести секретный ключ предъявителя на устройстве 1005 приема. В одном варианте осуществления устройство 1005 приема может дополнительно отображать на стадии 1012 предварительно определенный вспомогательный параметр предъявляющей стороне 1002 взаимодействия для дополнительной корреляции взаимодействия и установления соответствия между сообщением устройства приема и сообщением устройства предъявления.

На стадии 1017 секретный ключ получают посредством устройства 1005 приема. В одном варианте осуществления предъявляющая сторона 1002 взаимодействия использует клавиатуру для ввода секретного ключа на устройстве 1005 приема. В другом варианте осуществления предъявляющая сторона 1002 взаимодействия может использовать прибор для передачи секретного ключа на устройство 1005 приема.

Затем на стадии 1019 устройство 1005 приема передает сообщение устройства приема на сервер 1001, разрешая выдачу характерного набора (наборов) идентификационных данных, связанного с предъявляющей стороной 1003 взаимодействия, на оборудование получателя, разрешенное предъявляющей стороной 1002 взаимодействия. Сообщение устройства приема содержит секретный ключ предъявителя, полученный на стадии 1017, и одноразовый общий ключ, сгенерированный на стадии 1012. Сообщение устройства приема также может содержать идентификатор, относящийся к принимающей стороне взаимодействия, если он извлечен после стадии 1012, и любые вспомогательные предварительно определенные параметры, если они захвачены после стадии 1012.

На стадии 1018 устройство 1003 предъявления передает сообщение устройства предъявления на сервер 1001, обеспечивая извлечение характерного набора (наборов) идентификационных данных, связанного с предъявляющей стороной 1002 взаимодействия, из места хранения, идентифицированного предъявляющей стороной 1002 взаимодействия. Сообщение устройства предъявления содержит идентификатор предъявителя, извлеченный на стадии 1013, и одноразовый общий ключ, полученный на стадии 1015. Сообщение устройства предъявления также может содержать условное название, соответствующее выбранному набору идентификационных данных, если оно было перечислено на стадии 1013 и выбрано на стадии 1016, и также может содержать любые предварительно определенные вспомогательные параметры, если они были захвачены после стадии 1016.

На стадии 1020 сервер 1001 ищет соответствие между принятыми сообщениями устройства приема и принятыми сообщениями устройства предъявления путем поиска соответствия между одноразовым общим ключом, содержащимся в сообщениях устройства приема, и одноразовым общим ключом, содер-

жащимся в сообщениях устройства предъявления. В некоторых вариантах осуществления сообщению устройства приема и/или сообщению устройства предъявления может быть назначен период достоверности 1020. Если сообщение устройства приема и сообщение устройства предъявления не соответствуют друг другу в течение назначенного периода достоверности, взаимодействие прекращается и считается завершенным, делая дальнейшие процессы лишними. Если взаимодействие прекращается и завершается, делая дальнейшие процессы лишними, данные, относящиеся к взаимодействию (т.е. сообщения взаимодействующих сторон), могут быть удалены из системы, высвобождая ресурсы для обработки других принятых разрешений. В других вариантах осуществления значение предварительно определенных вспомогательных параметров может содержаться в сообщении устройства приема на стадии 1019 и сообщении устройства предъявления на стадии 1018. Если это так, значение используют в дополнение к общему ключу в качестве предварительно определенного вспомогательного параметра для поиска соответствия между сообщением устройства приема и сообщением устройства предъявления на стадии 1020.

На стадии 1021 и в случае нахождения соответствия на стадии 1020 сервер 1001 инициирует поиск путем связывания 1021 идентификатора предъявителя, содержащегося в сообщении устройства предъявления, и секретного ключа, содержащегося в сообщении устройства приема, при этом общий ключ, содержащийся в сообщении устройства предъявления, является таким же, что и общий ключ, содержащийся в сообщении устройства приема, согласно стадии 1020. Если на стадии 1020 соответствие не обнаружено, то способ не переходит к стадии 1021, и сервер 1001 может вернуть сообщение соответственно на устройство 1005 приема или устройство 1003 предъявления.

На стадии 1022 сервер 1001 выполняет поиск целевой записи в группе записей предъявителя, содержащей идентификатор предъявителя, находящийся в соответствующем сообщении устройства предъявления, и секретный ключ, находящийся в соответствующем сообщении устройства приема. В одном варианте осуществления и в случае 1022, если условное название, соответствующее идентификатору предъявителя, содержится в сообщении устройства предъявления согласно стадии 1018, условное название также используется для установления 1022 целевой записи, содержащей указанное условное название, в дополнение к идентификатору предъявителя и секретному ключу предъявляющей стороны 1002 взаимодействия.

На стадии 1023 и в случае, если запись, содержащая идентификатор предъявителя и секретный ключ предъявителя, найдена на стадии 1022, поиск продолжается путем идентификации 1023 отметки, связанной с целевой записью, найденной на стадии 1022, при этом отметка относится к набору идентификационных данных, связанных с предъявляющей стороной 1002 взаимодействия (в одном варианте осуществления рассматриваемый набор идентификационных данных может представлять собой набор идентификационных данных, связанных с условным названием, выбранным предъявляющей стороной 1002 взаимодействия на этапе 1022). В одном варианте осуществления идентифицированная отметка содержит считанные данные, содержащие идентификационные данные, связанные с предъявляющей стороной 1002 взаимодействия. В другом варианте осуществления идентифицированная отметка содержит указатель, обозначающий место расположения идентификационных данных, связанных с предъявляющей стороной 1002 взаимодействия. В случае, если запись, содержащая идентификатор предъявителя и секретный ключ предъявителя, не найдена на этапе 1022, то процесс не продолжается стадией 1023, и сервер 1001 может вернуть сообщение соответственно на устройство 1005 приема и/или устройство 1003 предъявления.

На стадии 1024 поиск завершается путем разрешения на извлечение считанных данных идентификационных данных, связанных с предъявляющей стороной 1002 взаимодействия, из места хранения, идентифицированного на стадии 1023, и разрешения выдачи считанных данных идентификационных данных, связанных с предъявляющей стороной взаимодействия, на оборудование получателя, разрешенное предъявляющей стороной 1002 взаимодействия.

На стадии 1025 считанные данные извлекают из места хранения, указанного предъявляющей стороной 1002 взаимодействия. В одном варианте осуществления считанные данные хранят и извлекают 1025 из управляющего сервера, выполненного с возможностью осуществления стадий 1020-1024 предложенного способа. В другом варианте осуществления считанные данные хранят и извлекают 1025 из другого сервера, отличного от управляющего сервера, выполненного с возможностью осуществления стадий 1020-1024 предложенного способа.

На стадии 1026 считанные данные идентификационных данных выдают 1026 на оборудование получателя, разрешенное предъявляющей стороной 1002 взаимодействия. В одном варианте осуществления считанные данные выдают и отправляют на конечную точку 1004 сети. В другом варианте осуществления считанные данные выдают и отправляют на устройство 1005 приема.

Согласно фиг. 10 и в результате событий после стадий 1027 и 1028 сообщение возвращают посредством сервера 1001 на устройство 1003 предъявления для предъявляющей стороны 1002 взаимодействия, указывая, были ли считанные данные извлечены в результате идентификации и выданы в результате разрешения предъявляющей стороной 1002 взаимодействия; в таких дополнительных вариантах осуществления на сервере 1001 хранится запись, в которой перечислены статусы событий, происходящих между стадиями 1020 и 1024, и ее может просмотреть предъявляющая сторона 1002 взаимодействия на устрой-

стве 1003 предъявления.

Варианты осуществления в настоящем изобретении, описанные со ссылкой на графические материалы, содержат вычислительное устройство и/или способы, выполняемые в вычислительном устройстве. Однако настоящее изобретение также распространяется на компьютерные программы, в частности компьютерные программы, хранящиеся на или в носителе информации, выполненном с возможностью практической реализации настоящего изобретения. Программа может быть представлена в виде программного кода, объектного кода или кода, представляющего собой среднее между программным и объектным кодом, например, в частично скомпилированном формате или в любом другом формате, подходящем для использования при реализации способа согласно настоящему изобретению. Носитель информации может содержать носитель данных, такой как ROM, например CD ROM, или магнитный носитель информации, например дискета или жесткий диск. Носитель информации может представлять собой электрический или оптический сигнал, который может быть передан по электрическому или оптическому кабелю, или по радио, или с помощью других средств.

Слова "содержит/содержащий" и слова "имеющий/включающий" при использовании в настоящем документе со ссылкой на настоящее изобретение предназначены для указания наличия обозначенных признаков, целых чисел, этапов или компонентов, но не исключают наличия или добавления одного или более других признаков, целых чисел, этапов, компонентов или их групп.

Следует понимать, что определенные признаки настоящего изобретения, которые для простоты изложения описаны в контексте отдельных вариантов осуществления, также могут быть предоставлены в комбинации в одном варианте осуществления. И наоборот, различные признаки настоящего изобретения, которые для краткости описаны в контексте одного варианта осуществления, также могут быть предоставлены отдельно или в любой подходящей комбинации.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система (100) контроля передачи по меньшей мере одного набора контролируемых идентификационных данных, соответствующих предъявителю, от сервера на конечную точку сети, причем указанная система содержит

по меньшей мере одну конечную точку сети;

устройство (109) приема, содержащее процессор устройства приема, интерфейс связи устройства приема, запоминающее устройство устройства приема и по меньшей мере одну из консоли ввода устройства приема и консоли вывода устройства приема, выполненное с возможностью отправки сообщения (104) устройства приема, причем указанное сообщение устройства приема содержит полученный секретный ключ (109a), относящийся к указанному предъявителю, и одноразовый общий ключ (109b);

устройство (108) предъявления, содержащее процессор устройства предъявления, интерфейс связи устройства предъявления, запоминающее устройство устройства предъявления и по меньшей мере одну из консоли ввода устройства предъявления и консоли вывода устройства предъявления, выполненное с возможностью отправки сообщения (105) устройства предъявления, причем указанное сообщение устройства предъявления содержит полученный идентификатор (108a) предъявителя, относящийся к указанному предъявителю, и указанный одноразовый общий ключ (108b);

по меньшей мере один сервер, который содержит процессор сервера, по меньшей мере один интерфейс связи сервера и запоминающее устройство сервера, хранящее:

(i) по меньшей мере одну отметку (103), относящуюся к указанному по меньшей мере одному набору контролируемых идентификационных данных, соответствующих предъявителю,

(ii) причем каждая отметка связана по меньшей мере с одной записью (102), причем запись относится к любому предъявителю и содержит записанный идентификатор предъявителя и записанный секретный ключ, соответствующий записанному идентификатору предъявителя;

причем указанный по меньшей мере один сервер выполнен с возможностью:

a) получения указанного сообщения (104) устройства приема;

b) получения указанного сообщения (105) устройства предъявления;

c) поиска соответствия между указанным одноразовым общим ключом (109b), содержащимся в указанном сообщении (104) устройства приема, и указанным одноразовым общим ключом (108b), содержащимся в указанном сообщении (105) устройства предъявления;

d) инициации поиска целевой записи путем связывания указанного полученного секретного ключа в указанном сообщении (104) устройства приема с указанным полученным идентификатором предъявителя в указанном сообщении (105) устройства предъявления, причем как указанное сообщение устройства приема, так и указанное сообщение устройства предъявления содержат одинаковый одноразовый общий ключ (108b, 109b);

e) выполнения поиска указанной целевой записи, которая содержит записанный секретный ключ и записанный идентификатор предъявителя, которые являются такими же, как указанный полученный секретный ключ (109a) и указанный полученный идентификатор (108a) предъявителя;

f) завершения поиска путем идентификации отметки (103), связанной с указанной целевой записью;

г) обеспечения извлечения указанного по меньшей мере одного набора контролируемых идентификационных данных, относящихся к указанной отметке (103), и обеспечения выдачи указанного по меньшей мере одного набора контролируемых идентификационных данных на указанную конечную точку (110) сети, причем указанная конечная точка сети является разрешенным получателем указанного по меньшей мере одного набора контролируемых идентификационных данных, соответствующих предъявителю.

2. Система по п.1, отличающаяся тем, что указанный по меньшей мере один сервер является управляющим сервером (101).

3. Система по п.2, отличающаяся тем, что управляющий сервер (101) дополнительно выполнен с возможностью генерирования указанного одноразового общего ключа и предоставления доступа к нему на устройстве (109) приема.

4. Система по п.2, отличающаяся тем, что указанное устройство приема дополнительно выполнено с возможностью генерирования указанного одноразового общего ключа, получения указанного полученного секретного ключа (109а) от указанного предъявителя и передачи указанного сообщения устройства приема на указанный управляющий сервер (101).

5. Система по п.3, отличающаяся тем, что указанное устройство предъявления дополнительно выполнено с возможностью получения указанного одноразового общего ключа от указанного устройства (109) приема, извлечения указанного полученного идентификатора предъявителя из запоминающего устройства указанного устройства предъявления и передачи указанного сообщения (105) устройства предъявления на указанный управляющий сервер (101).

6. Система по любому из пп.1-5, отличающаяся тем, что указанная запись, содержащая указанный записанный идентификатор предъявителя и указанный записанный секретный ключ, дополнительно содержит условное название, соответствующее идентификатору предъявителя и связанное с указанной отметкой (103), относящейся к указанному по меньшей мере одному набору контролируемых идентификационных данных.

7. Система по любому из пп.1-6, отличающаяся тем, что указанное сообщение устройства предъявления дополнительно содержит условное название, соответствующее указанному полученному идентификатору предъявителя и связанное с указанной отметкой (103), относящейся к указанному по меньшей мере одному набору контролируемых идентификационных данных, и при этом при указанном поиске указанной целевой записи дополнительно применяется указанное условное название, содержащееся в указанном сообщении (105) устройства предъявления, для поиска указанной целевой записи, содержащей указанное условное название в дополнение к указанному полученному идентификатору (108а) предъявителя и указанному полученному секретному ключу.

8. Система по любому из пп.1-7, отличающаяся тем, что указанная конечная точка сети содержит указанное устройство (109) приема и выполнена в виде назначенного получателя одного или более типов указанного по меньшей мере одного набора контролируемых идентификационных данных.

9. Система по любому из пп.1-7, отличающаяся тем, что указанная конечная точка сети связана с указанным устройством приема и выполнена в виде назначенного получателя одного или более типов указанного по меньшей мере одного набора контролируемых идентификационных данных.

10. Система по п.2, отличающаяся тем, что указанный по меньшей мере один набор контролируемых идентификационных данных содержит отметку в указанной целевой записи (102) на указанном управляющем сервере (101).

11. Система по п.1, отличающаяся тем, что указанный по меньшей мере один сервер содержит управляющий сервер (101) и сервер, который отличается от указанного управляющего сервера, при этом указанный по меньшей мере один набор контролируемых идентификационных данных содержит отметку на сервере, который отличается от указанного управляющего сервера, при этом отметка на сервере, который отличается от указанного управляющего сервера, связана с указанной целевой записью на указанном управляющем сервере (101).

12. Система по любому из пп.1-11, отличающаяся тем, что указанному сообщению (104) устройства приема назначен период достоверности, и причем этап с) дополнительно включает установление того, истек ли указанный период достоверности.

13. Система по любому из пп.1-11, отличающаяся тем, что указанному сообщению (105) устройства предъявления назначен период достоверности, и причем этап с) дополнительно включает установление того, истек ли указанный период достоверности.

14. Система по любому из пп.1-11, отличающаяся тем, что указанному одноразовому общему ключу назначен период достоверности, и причем этап с) дополнительно включает установление того, истек ли указанный период достоверности.

15. Система по п.14, отличающаяся тем, что указанный одноразовый общий ключ является уникальным в течение длительности указанного периода достоверности.

16. Система по любому из пп.1-15, отличающаяся тем, что указанное сообщение (104) устройства приема дополнительно содержит один или более предварительно определенных вспомогательных параметров, и указанное сообщение устройства предъявления также дополнительно содержит указанный

один или более предварительно определенных вспомогательных параметров.

17. Система по п.16, если зависит от любого из пп.2-5, отличающаяся тем, что указанный управляющий сервер (101) ищет соответствие между по меньшей мере одним из указанных предварительно определенных вспомогательных параметров из указанного сообщения (105) устройства предъявления и указанным соответствующим предварительно определенным параметром (указанными соответствующими предварительно определенными параметрами) из указанного сообщения (104) устройства приема для дополнительного обеспечения по меньшей мере одного из корреляции и подтверждения.

18. Система по любому из пп.2-5, отличающаяся тем, что если указанные записи содержат отметки по меньшей мере одного набора контролируемых идентификационных данных на указанном управляющем сервере (101), этапы f) и g) выполняют на указанном управляющем сервере, и передачу указанного по меньшей мере одного набора контролируемых идентификационных данных выполняют из указанного управляющего сервера.

19. Система по любому из пп.2-5, отличающаяся тем, что если указанные записи содержат отметки по меньшей мере одного набора контролируемых идентификационных данных на сервере, который отличается от указанного управляющего сервера, этапы f) и g) выполняют на указанном другом сервере, и передачу указанного по меньшей мере одного набора контролируемых идентификационных данных выполняют с помощью одного из указанного управляющего сервера и указанного другого сервера.

20. Система по любому из пп.2-5, отличающаяся тем, что если соответствие между указанным сообщением (104) устройства приема и сообщением (105) устройства предъявления не найдено на указанном управляющем сервере (101), указанный управляющий сервер прекращает выполнение дальнейших настроенных действий и записывает статус событий в указанном месте.

21. Система по любому из пп.2-5, отличающаяся тем, что если целевая запись не найдена на указанном управляющем сервере (101), указанный управляющий сервер прекращает выполнение дальнейших настроенных действий и записывает статус событий в указанном месте.

22. Система по любому из пп.2-5, отличающаяся тем, что указанный управляющий сервер (101) дополнительно выполнен с возможностью записи статуса происходящих событий и передачи указанного статуса по меньшей мере на одно из указанного устройства (109) приема и указанного устройства (108) предъявления.

23. Система по любому из пп.1-22, отличающаяся тем, что каждая конечная точка (110) сети содержит процессор конечной точки сети, интерфейс связи конечной точки сети, запоминающее устройство конечной точки сети и по меньшей мере одну из консоли ввода конечной точки сети и консоли вывода конечной точки сети.

24. Система по любому из пп.1-23, отличающаяся тем, что система выполнена с возможностью работы по сети (106, 107, 111) связи.

25. Способ контроля передачи по меньшей мере одного набора контролируемых идентификационных данных, соответствующих предъявителю, по меньшей мере от одного сервера на конечную точку (110) сети, причем указанный способ включает следующие этапы, выполняемые по меньшей мере одним сервером:

(a) получения от устройства приема, содержащего процессор устройства приема, запоминающее устройство устройства приема, по меньшей мере одну из консоли ввода устройства приема и консоли вывода устройства приема и интерфейс связи устройства приема, сообщения (104) устройства приема, причем указанное сообщение содержит полученный секретный ключ (109a), относящийся к указанному предъявителю, и одноразовый общий ключ (109b);

(b) получения от устройства предъявления, содержащего процессор устройства предъявления, запоминающее устройство устройства предъявления, по меньшей мере одну из консоли ввода устройства предъявления и консоли вывода устройства предъявления и интерфейс связи устройства предъявления, сообщения (105) устройства предъявления, причем указанное сообщение содержит полученный идентификатор (108a) предъявителя, относящийся к указанному предъявителю, и одноразовый общий ключ (108b);

(c) поиска по меньшей мере одним процессором сервера по меньшей мере одного сервера соответствия между указанным одноразовым общим ключом (109b), содержащимся в указанном сообщении (104) устройства приема, и указанным одноразовым общим ключом (108b), содержащимся в указанном сообщении (105) устройства предъявления;

(d) инициации по меньшей мере одним процессором сервера поиска целевой записи путем связывания указанного полученного секретного ключа (109a) указанного сообщения (104) устройства приема с указанным полученным идентификатором (108a) предъявителя в указанном сообщении (105) устройства предъявления, причем как указанное сообщение устройства приема, так и указанное сообщение устройства предъявления содержат одинаковый одноразовый общий ключ (108b, 109b);

(e) выполнения по меньшей мере одним процессором сервера поиска целевой записи, содержащей записанный секретный ключ и записанный идентификатор предъявителя, которые являются такими же, как указанный полученный секретный ключ (109a) и указанный полученный идентификатор (108a) предъявителя;

(f) идентификации по меньшей мере одним процессором сервера отметки (103), связанной с указанной целевой записью, причем указанная отметка относится к указанному по меньшей мере одному набору контролируемых идентификационных данных, соответствующих предъявителю; и

(g) обеспечения по меньшей мере одним процессором сервера извлечения указанного по меньшей мере одного набора контролируемых идентификационных данных, относящихся к указанной отметке, и обеспечения выдачи указанного набора контролируемых идентификационных данных на указанную конечную точку (110) сети, причем указанная конечная точка является разрешенным получателем указанного по меньшей мере одного набора контролируемых идентификационных данных, соответствующих предъявителю.

26. Способ по п.25, отличающийся тем, что целевая запись дополнительно содержит условное название, соответствующее указанному полученному идентификатору (108a) предъявителя и связанное с указанной отметкой (103), относящейся к указанному по меньшей мере одному набору контролируемых идентификационных данных, и указанное сообщение (105) устройства предъявления дополнительно содержит условное название, соответствующее полученному указанному идентификатору (108a) предъявителя и связанное с указанной отметкой, относящейся к указанному по меньшей мере одному набору контролируемых идентификационных данных, и причем этап (e) дополнительно включает установление соответствия между соответствующими условными названиями указанной записи и указанным сообщением устройства предъявления.

27. Способ по п.25 или 26, отличающийся тем, что указанный по меньшей мере один сервер содержит управляющий сервер (101) и этапы (a)-(g) выполняют на нем.

28. Способ по п.25 или 26, отличающийся тем, что указанный по меньшей мере один сервер содержит управляющий сервер (101) и сервер, который отличается от указанного управляющего сервера, и тем, что указанный по меньшей мере один набор контролируемых идентификационных данных содержит отметку на указанном сервере, который отличается от указанного управляющего сервера (101), причем указанная отметка связана с указанной целевой записью, и причем этап идентификации набора идентификационных данных выполняют на указанном другом сервере, и причем этапы (e)-(g) выполняют на одном из указанного управляющего сервера (101) и указанного сервера, который отличается от указанного управляющего сервера.

29. Способ по любому из пп.25-28, отличающийся тем, что дополнительно включает назначение периода достоверности по меньшей мере одному из указанного сообщения (104) устройства приема, указанного сообщения (105) устройства предъявления и указанного одноразового общего ключа, и этап (c) дополнительно включает установление того, истек ли указанный период достоверности.

30. Способ по п.29, отличающийся тем, что указанный одноразовый общий ключ является уникальным в течение длительности указанного периода достоверности.

31. Способ по любому из пп.25-29, отличающийся тем, что каждое из указанного сообщения (105) устройства предъявления и указанного сообщения (104) устройства приема дополнительно содержит один или более предварительно определенных вспомогательных параметров, и причем этап (c) дополнительно включает поиск соответствия между по меньшей мере одним из указанных предварительно определенных вспомогательных параметров в указанном сообщении устройства предъявления и по меньшей мере одним из соответствующих предварительно определенных вспомогательных параметров в указанном сообщении устройства приема.

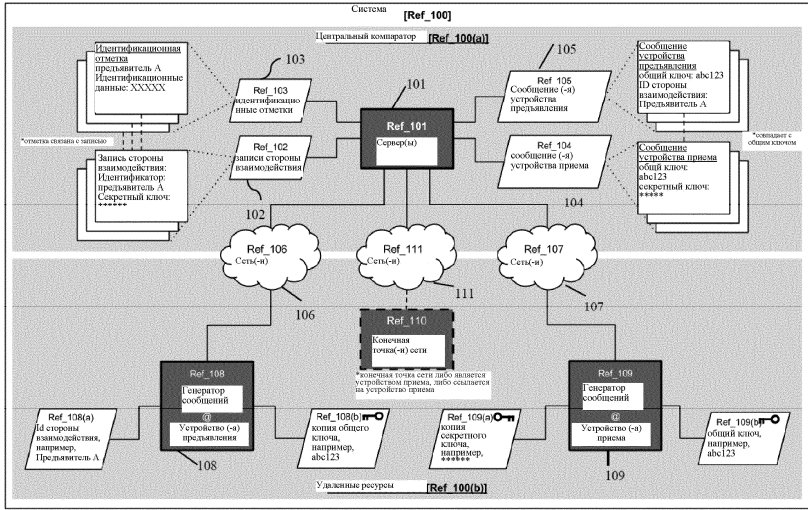
32. Способ по п.27, отличающийся тем, что если указанные записи содержат отметки по меньшей мере одного набора контролируемых идентификационных данных на указанном управляющем сервере (101), выполняют этапы (f) и (g) на указанном управляющем сервере, и способ дополнительно включает выдачу указанного по меньшей мере одного набора контролируемых идентификационных данных из указанного управляющего сервера.

33. Способ по п.25 или 26, отличающийся тем, что указанный по меньшей мере один сервер содержит управляющий сервер (101), и если указанные записи содержат отметки по меньшей мере одного набора контролируемых идентификационных данных на сервере, который отличается от указанного управляющего сервера (101), выполняют этапы (f) и (g) на указанном другом сервере, причем способ дополнительно включает выдачу указанного по меньшей мере одного набора контролируемых идентификационных данных из одного из указанного управляющего сервера и указанного другого сервера.

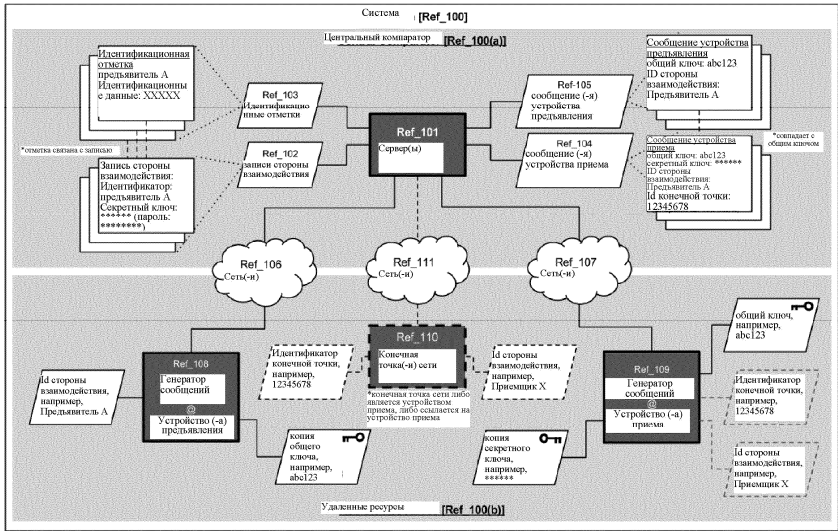
34. Способ по п.27 или 28, отличающийся тем, что если не найдено соответствия между указанным сообщением (104) устройства приема и сообщением (105) устройства предъявления, прекращают выполнение дальнейших настроенных действий и записывают статус событий в указанном управляющем сервере (101).

35. Способ по п.27 или 28, отличающийся тем, что если целевая запись не найдена, прекращают выполнение дальнейших настроенных действий и записывают статус событий в указанном управляющем сервере (101).

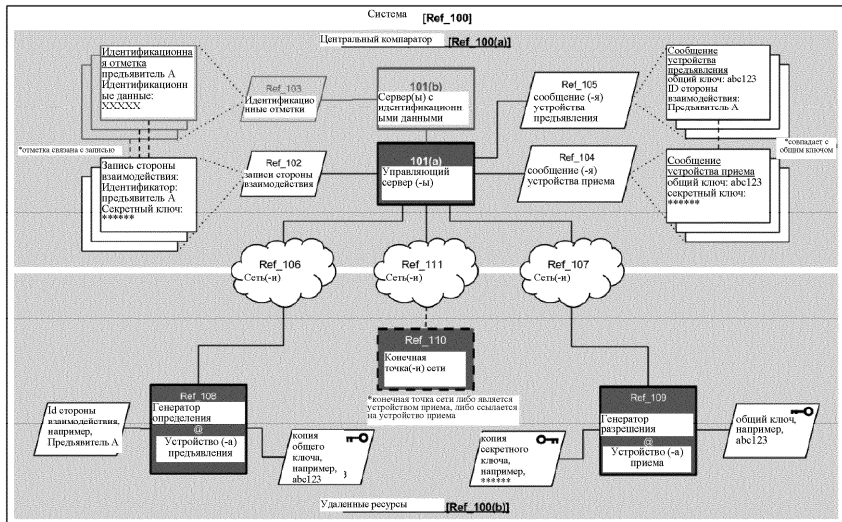
36. Способ по п.27 или 28, отличающийся тем, что дополнительно включает запись статуса событий в указанном управляющем сервере (101) и передачу статуса по меньшей мере на одно из указанного устройства (109) приема и указанного устройства (108) предъявления.



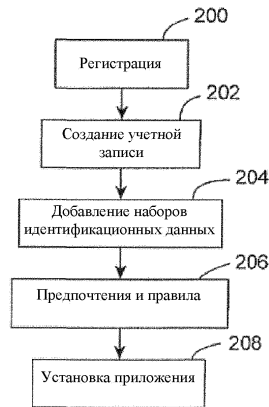
ФИГ. 1



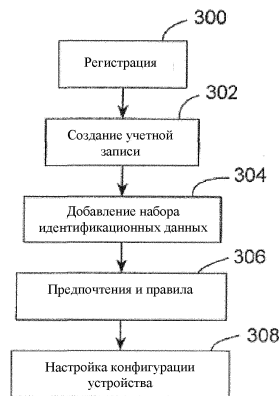
Фиг. 1А



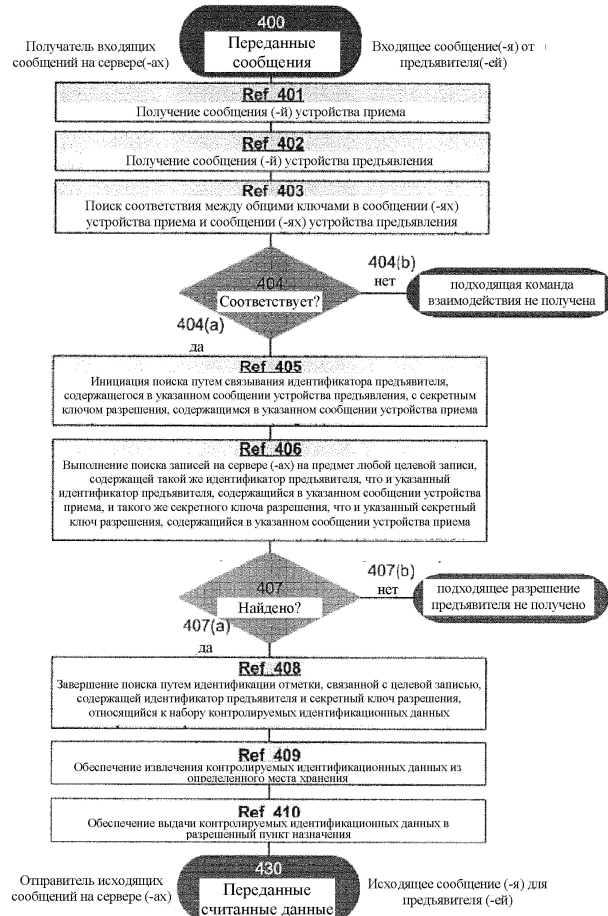
ФИГ. 1В



Фиг. 2



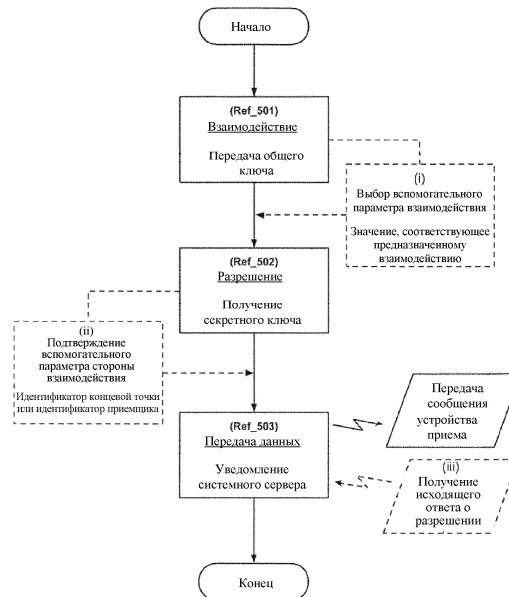
Фиг. 3



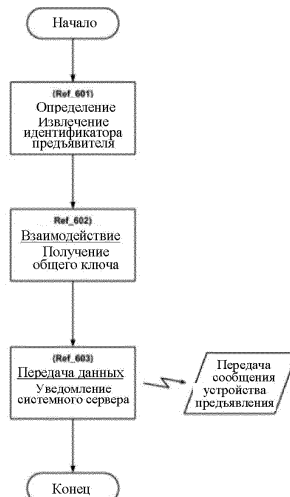
Фиг. 4



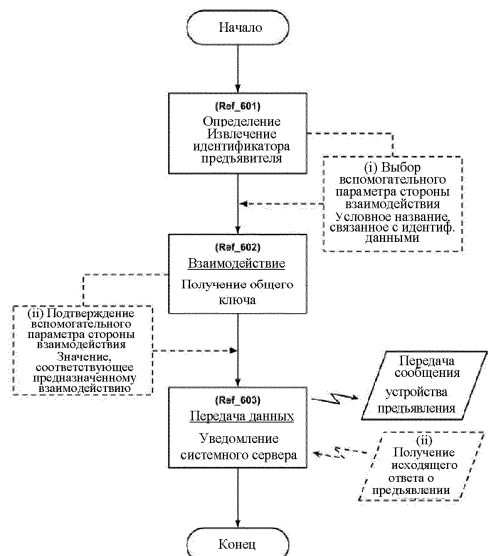
Фиг. 5А



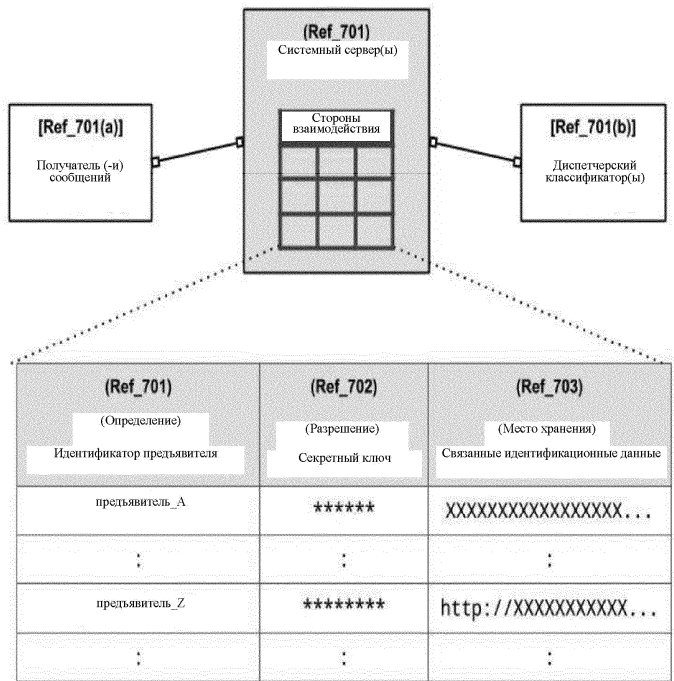
Фиг. 5В



Фиг. 6А



Фиг. 6В



Фиг. 7



Фиг. 7А

Ref_701 (определение) идентификатор стороны взаимодействия	Ref_702 (разрешение) секретный ключ	Ref_703 (место хранения) связанные идентификационные данные
8c48847bcc...	s2YisvHPL+...	%B555555...
⋮	⋮	⋮
9415bfefcc...	0a51YaQqR9...	P<XXXBLOGGS<<JOHN...
d299997ce5...	tnemmXw3Qp...	%B444444...
c4345d0f05...	uGkM35SWPs...	%Z999999...
⋮	⋮	⋮
c4e417c0f9...	LBucbRQmIP...	https://registry7...

Фиг. 7В

(Ref_701) (определение) идентификатор стороны взаимодействия	(Ref_702) (разрешение) секретный ключ	(Ref_701) (определение) идентификатор стороны взаимодействия	(Ref_703) (место хранения) связанные идентификацион ные данные
предъявитель А	*****	предъявитель А	XXXXXXXXXX...
⋮	⋮	⋮	⋮
предъявитель F	*****	предъявитель F	XXXXXXXXXX...
предъявитель С	*****	предъявитель С	XXXXXXXXXX...
предъявитель Н	*****	предъявитель Н	XXXXXXXXXX...
⋮	⋮	⋮	⋮
предъявитель В	*****	предъявитель В	XXXXXXXXXX...

Фиг. 7С

Ref_701 (определение) идентификатор стороны взаимодействия	Ref_702 (разрешение) секретный ключ	Ref_701 (определение) идентификатор стороны взаимодействия	Ref_703 (место хранения) связанные идентификацион ные данные
8c48847bcc...	s2YisvHPL+...	8c48847bcc...	%B555555...
⋮	⋮	⋮	⋮
9415bfefcc...	0a51YaQqR9...	9415bfefcc...	P<XXXBLOGG...
d299997ce5...	tnemmXw3Qp...	d299997ce5...	%B444444...
c4345d0f05...	uGkM35SWPs...	c4345d0f05...	%Z999999...
⋮	⋮	⋮	⋮
c4e417c0f9...	LBucbRQmIP...	c4e417c0f9...	https://re...

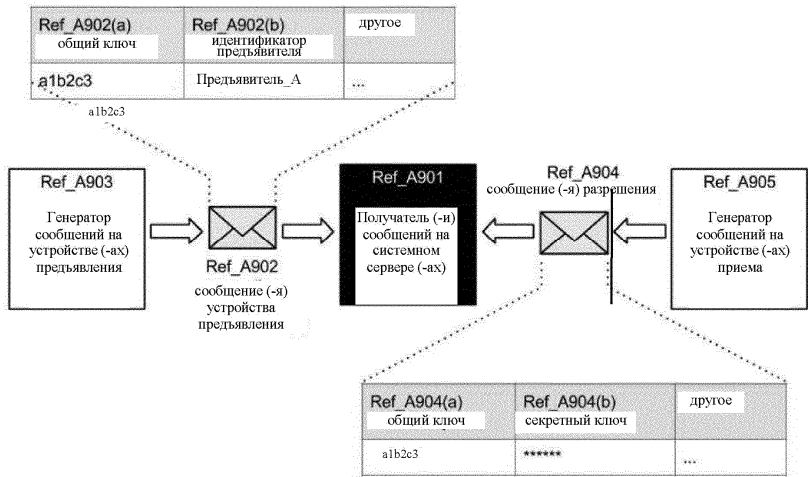
Фиг. 7D

Ref_S201 (определение) идентификатор стороны взаимодействия	Ref_S204 (различение) связанное условное название	Ref_S202 (разрешение) секретный ключ	Ref_S203 (место хранения) связанные идентификацион ные данные
предъявитель А	a3	*****	XXXXXXXXXXXX...
предъявитель А	a4	*****	XXXXXXXXXXXX...
предъявитель А	a6	*****	XXXXXXXXXXXX...
предъявитель F		*****	XXXXXXXXXXXX...
предъявитель С	c8	*****	XXXXXXXXXXXX...
предъявитель С	c10	*****	XXXXXXXXXXXX...
предъявитель Z		*****	XXXXXXXXXXXX...
предъявитель В	b55	*****	XXXXXXXXXXXX...
предъявитель В	b41	*****	XXXXXXXXXXXX...

Фиг. 7Е



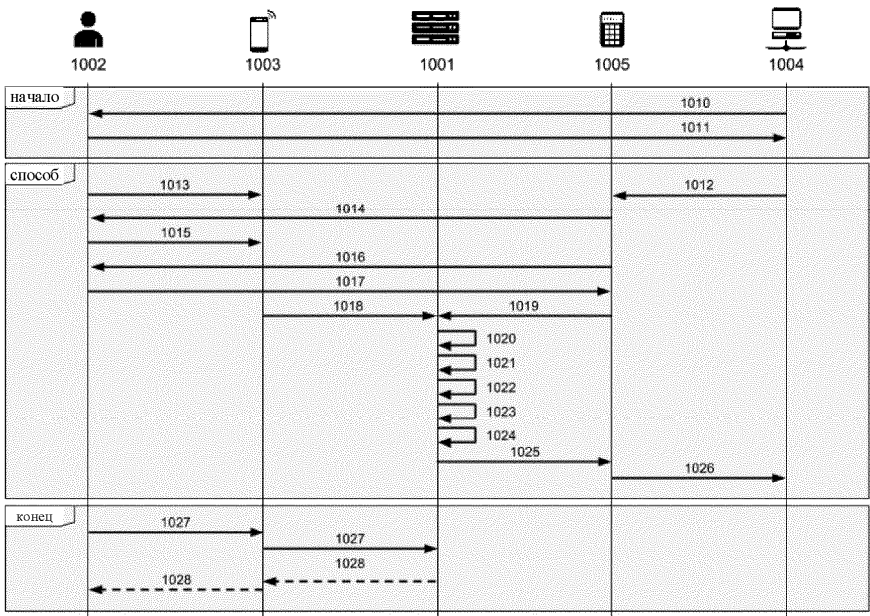
Фиг. 8



Фиг. 9А



Фиг. 9В



Фиг. 10

