РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 518 924** (13) **C2**

(51) МПК
H04W 8/00 (2009.01)
G06F 21/30 (2013.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2011144919/08, 28.10.2011**

(24) Дата начала отсчета срока действия патента:
28.10.2011

Приоритет(ы):
(30) Конвенционный приоритет:
28.10.2010 US 61/407,866;
05.04.2011 US 13/080,521

(43) Дата публикации заявки: **10.05.2013** Бюл. № **13**

(45) Опубликовано: **10.06.2014** Бюл. № **16**

(56) Список документов, цитированных в отчете о поиске: **US 2009/0205028 A1, 13.08.2009. US 2009/0271850 A1, 29.10.2009. US 2008/0016504 A1, 17.01.2008. RU 2008118949 A, 20.11.2009. RU 2006134030 A, 27.03.2008. US 2010/0062808 A1, 11.03.2010. CN 101625645 A, 13.01.2010. Michael Kasper et al., "Subscriber Authentication in mobile cellular Networks with virtual software SIM Credentials using Trusted** (см. прод.)

Адрес для переписки:
197101, Санкт-Петербург, а/я 128, "АРС-ПАТЕНТ"

(72) Автор(ы):
ШЕЛЛ Стефан В. (US),
ФОН ХАУК Джеррольд (US)

(73) Патентообладатель(и):
ЭППЛ ИНК. (US)

(54) БЕСПРОВОДНОЕ УСТРОЙСТВО, СПОСОБ ЗАПРОСА ПОЛЬЗОВАТЕЛЬСКОГО КЛИЕНТА УПРАВЛЕНИЯ ДОСТУПОМ И СПОСОБ ВЫПОЛНЕНИЯ КЛИЕНТА УПРАВЛЕНИЯ ДОСТУПОМ

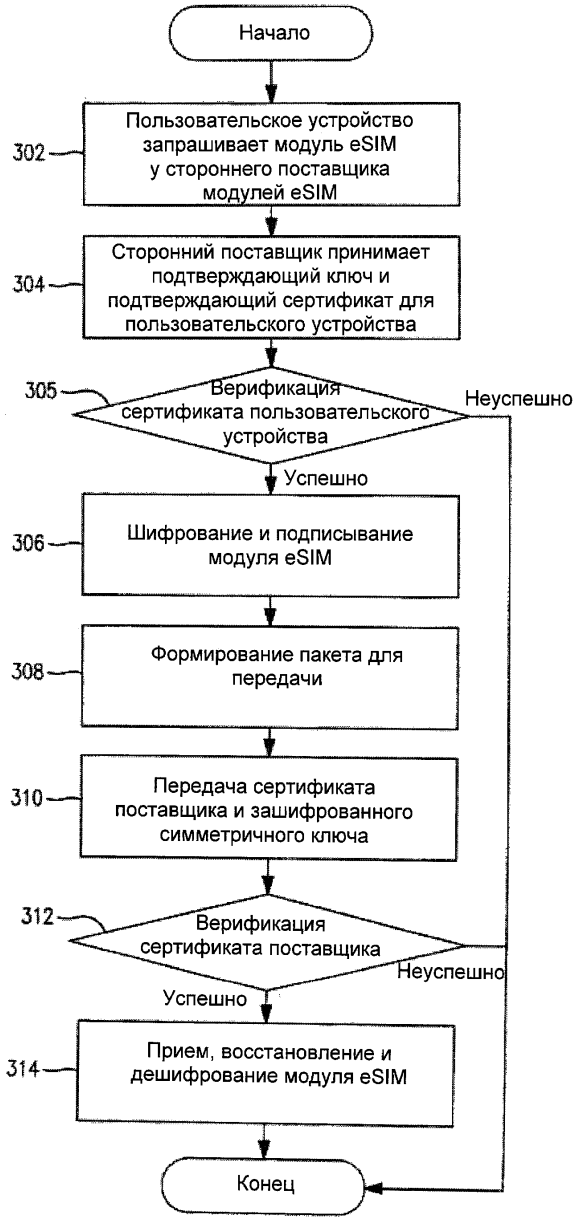
(57) Реферат:

Изобретение относится к беспроводной связи, а именно к способу для безопасной передачи клиента управления доступом. Техническим результатом является повышение безопасности. Способ содержит запрос пользовательского клиента управления доступом из беспроводной сети, при этом запрос связан с первым подтверждающим сертификатом; прием пользовательского клиента управления доступом и второго подтверждающего сертификата, при этом первый и второй подтверждающий сертификаты выданы доверенной структурой; и сохранение пользовательского клиента управления доступом в безопасном элементе, если второй подтверждающий сертификат действителен; причем пользовательский клиент управления доступом сохраняют в индивидуальном сегменте из числа множества сегментов, из которых состоит безопасный элемент, и последующие модификации сохраненного пользовательского клиента управления доступом могут быть выполнены только с использованием второго подтверждающего сертификата; а доступ к беспроводной сети ограничен (i) доступом посредством пользовательского клиента управления доступом и (ii) запросами пользовательских клиентов управления доступом.

RU 2518924 C2

RU 2518924 C2

3 н. и 19 з.п. ф-лы, 8 ил.



ФИГ.3

(56) (продолжение):
Computing", Advanced Communication Technology, 2008, ICACT. 10th International Conference on, 03.2008, найдено в Интернете по адресу "http://www.researchgate.net/publication/ 4325291_Subscriber_Authentication_in_Cellular_Networks_with_Trusted_Virtual_SIMs"

RU 2518924 C2

RU 2518924 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 518 924** (13) **C2**

(51) Int. Cl.
H04W 8/00 (2009.01)
G06F 21/30 (2013.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2011144919/08, 28.10.2011**

(24) Effective date for property rights:
28.10.2011

Priority:
(30) Convention priority:
28.10.2010 US 61/407,866;
05.04.2011 US 13/080,521

(43) Application published: **10.05.2013** Bull. № **13**

(45) Date of publication: **10.06.2014** Bull. № **16**

Mail address:
197101, Sankt-Peterburg, a/ja 128, "ARS-PATENT"

(72) Inventor(s):
ShELL Stefan V. (US),
FON KhAUK Dzherrol'd (US)

(73) Proprietor(s):
APPLE INC. (US)

RU 2518924 C2

(54) WIRELESS DEVICE, USER ACCESS CONTROL CLIENT REQUEST METHOD AND ACCESS CONTROL CLIENT METHOD

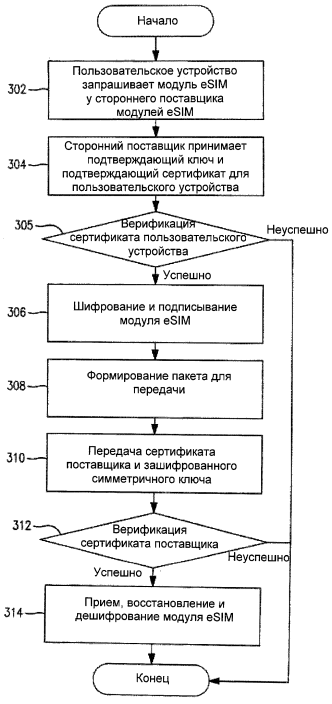
(57) Abstract:

FIELD: radio engineering, communication.

SUBSTANCE: invention relates to wireless communication and specifically to a method for secure access control client transmission. The method includes requesting a user access control client from a wireless network, wherein the request is associated with a first acknowledgement certificate; receiving the user access control client and a second acknowledgement certificate, wherein the first and second acknowledgement certificates are issued by a trusted entity; and storing the user access control client in a safe element if the second acknowledgement certificate is valid; wherein the user access control client is stored in a particular segment from a plurality of segments making up the safe element, and subsequent modifications of the stored user access control client can be performed only using the second acknowledgement certificate; and access to the wireless network is limited (i) by access through the user access control client and (ii) user access control client requests.

EFFECT: improved security.

22 cl, 8 dwg



ФИГ.3

RU 2518924 C2

Область техники, к которой относится изобретение

Настоящее изобретение относится в целом к области беспроводной связи и сетей передачи данных. В частности, настоящее изобретение в одном примерном аспекте относится к способу и устройству для безопасной модификации, сохранения и выполнения структуры или клиента управления доступом.

Уровень техники

Управление доступом требуется для безопасной связи в большинстве систем беспроводной радиосвязи из уровня техники. Например, простая схема управления доступом может включать: (i) верификацию идентификации осуществляющей связь стороны и (ii) выделение уровня доступа, соразмерного верифицированной идентификации. В контексте примерной системы сотовой связи, например универсальной системы мобильной связи (Universal Mobile Telecommunications System, UMTS), управление доступом осуществляется посредством клиента управления доступом, называемого универсальным модулем идентификации абонента (Universal Subscriber Identity Module, USIM), выполняемого на физической универсальной карте с интегральной схемой (Universal Integrated Circuit Card, UICC). Клиент управления доступом USIM осуществляет аутентификацию абонента в сети сотовой связи UMTS. После успешной аутентификации абоненту разрешают доступ в сотовую сеть. Используемый в настоящем документе термин «клиент управления доступом» в целом относится к логической структуре, реализованной либо в аппаратном, либо в программном обеспечении с возможностью управления доступом первого устройства в сеть. Распространенные примеры клиентов управления доступом включают указанные выше универсальный модуль идентификации абонента (USIM), модуль идентификации абонента CDMA (CSIM), модуль идентификации мультимедийных служб протокола IP (ISIM), модуль идентификации абонента (SIM), удаляемый модуль идентификации абонента (RUIM) и т.п.

Как правило, модуль USIM (или в целом модуль SIM) осуществляет хорошо известную процедуру аутентификации и согласования ключа (AKA, Authentication and Key Agreement), в которой верифицируют и дешифруют применимые данные и программы для обеспечения безопасной инициализации. В частности, модуль USIM должен одновременно (i) успешно ответить на удаленный проверочный запрос для подтверждения своей идентификации оператору сети и (ii) передать проверочный запрос на верификацию идентификации сети.

Однако существующие модули идентификации абонента имеют множество недоработок и недостатков. Во-первых, программное обеспечение модуля идентификации абонента SIM жестко запрограммировано в физических карточных носителях UICC, и абоненту требуется новая карта UICC для изменения работы модуля идентификации абонента. Это может быть недостатком и для операторов сети мобильной связи, и для абонентов, например, если процедуры аутентификации «взломаны» (например, посредством враждебных хакерских атак), абоненту должна быть выделена новая карта UICC, при этом данный процесс является трудоемким и затратным. Кроме того, по причинам, описанным в настоящем документе ниже, физический модуль идентификации абонента признает только одну доверенную структуру, в частности оператора сети мобильной связи (MNO), с которым он может обеспечивать связь. Таким образом, в настоящее время отсутствует какой-либо способ для включения в систему программирования, осуществляемого после развертывания, за исключением использования существующей доверенной взаимосвязи между устройством и оператором сети мобильной связи. Например, сторонние разработчики модулей идентификации абонента, желающие предложить новое или обновленное программное обеспечение

модуля идентификации абонента, не имеют такой возможности из-за отсутствия гибкости физических карточных носителей модуля идентификации абонента, а также невозможности установления доверенной взаимосвязи между ними и модулем идентификации абонента. Этот критический момент управления существенно ограничивает количество потенциальных абонентов и возможности, предоставляемые поставщикам модулей идентификации абонента.

Таким образом, требуются новые решения для обеспечения распространения, осуществляемого после развертывания, и модификации модулей идентификации абонента. В идеале такие решения должны позволять мобильному устройству принимать и реализовывать изменения в работе модуля идентификации абонента, когда устройство находится в «поле» (после развертывания). Кроме того, требуемые способы и устройство должны поддерживать другие необходимые функции, в том числе такие как поддержка нескольких профилей модуля идентификации абонента, гибкость в работе, обновления и т.п.

Однако в целом указанные способы и устройство требуются для обеспечения безопасной модификации, сохранения и выполнения клиентов управления доступом. Требуются способы модификации работы клиента управления доступом для поддержки таких функций, как несколько профилей доступа абонента, безопасное обновление устройства, альтернативные способы для предоставления услуг абоненту и т.п. Кроме того, из-за важности управления доступом и возможности скрытого использования и хищения услуг главной задачей являются безопасные способы осуществления таких изменений.

Раскрытие изобретения

Указанные выше цели достигнуты в настоящем изобретении путем предложения улучшенного устройства и способов для безопасной модификации, сохранения и выполнения клиентов управления доступом.

В первом аспекте настоящего изобретения предлагается беспроводное устройство. В одном варианте осуществления устройство включает один или большее количество каналов беспроводной связи, обеспечивающих возможность осуществления связи с по меньшей мере одной сетью посредством клиента управления доступом, безопасный элемент, выполненный с возможностью хранения клиента управления доступом, интерфейс к безопасному элементу, включающий криптографический ключ и связанный с ним подтверждающий сертификат, вычислительное устройство и устройство хранения, соединенное с возможностью обмена данными с вычислительным устройством и содержащее выполняемые компьютером инструкции. По меньшей мере подмножество выполняемых компьютером инструкций дополнительно подразделено на один или большее количество сегментов.

В одном варианте указанные инструкции при выполнений вычислительным устройством посредством интерфейса передают запрос одного или большего количества компонентов для клиента управления доступом, относящегося к по меньшей мере одной сети, при этом запрос включает подтверждающий сертификат и криптографический ключ, принимают один или большее количество запрошенных компонентов, при этом указанные компоненты связаны со вторым подтверждающим сертификатом, верифицируют второй подтверждающий сертификат и в ответ на успешную верификацию второго подтверждающего сертификата загружают клиент управления доступом.

Во втором аспекте настоящего изобретения предлагается способ взаимной аутентификации. В одном варианте осуществления способ включает: запрос одного

или большего количества компонентов, при этом запрос связан с первым подтверждающим сертификатом, прием одного или большего количества компонентов и второго подтверждающего сертификата и загрузку одного или большего количества компонентов в случае, если второй подтверждающий сертификат действителен, причем первый и второй подтверждающий сертификаты выданы доверенной структурой.

В третьем аспекте настоящего изобретения предлагается способ выполнения клиента управления доступом. В одном варианте осуществления способ включает выполнение первой самозагружаемой операционной системы, которая выбирает безопасный сегмент, связанный лишь с одним клиентом управления доступом, верификацию безопасного сегмента, включающего одну общую операционную систему и один клиент управления доступом, и выполнение общей операционной системы, которая загружает один клиент управления доступом. Клиент управления доступом обладает возможностью аутентификации в сети, например внешней сотовой сети.

В четвертом аспекте настоящего изобретения предлагается мобильное устройство. В одном варианте осуществления мобильное устройство выполнено с возможностью запроса, приема и использования структуры данных виртуального или электронного модуля идентификации абонента с использованием архитектуры самозагружаемой операционной системы.

В пятом аспекте настоящего изобретения предлагается считываемое компьютером устройство. В одном варианте осуществления устройство включает носитель информации с по меньшей мере одной выполняющейся на нем компьютерной программой, причем указанная по меньшей мере одна программа обладает возможностью приема, обработки и предоставления запросов виртуальных или электронных модулей идентификации абонента с использованием самозагружаемой операционной системы.

В шестом аспекте настоящего изобретения предлагается система распространения среди пользователей виртуальных или электронных модулей идентификации абонента. В одном варианте осуществления система включает устройство для доставки компонентов операционной системы, поддерживающих передачу электронного модуля идентификации абонента по сети, например сети Интернет, или MAN, или WLAN.

Другие признаки и преимущества настоящего изобретения станут очевидны специалистам в данной области техники, ознакомленным с прилагаемыми чертежами и подробным описанием примерных вариантов осуществления, приведенным ниже.

Краткое описание чертежей

Фиг.1 представляет собой схему примера процедуры аутентификации и согласования ключа (АКА) с использованием модуля идентификации абонента из уровня техники.

Фиг.2 представляет собой логическую схему одного варианта осуществления способа назначения пары ключей устройства программной структуре (например, пользовательскому устройству (UE, терминалу пользователя) или стороннему поставщику программного обеспечения, поставщику модуля идентификации абонента и т.п.) в соответствии с изобретением.

Фиг.3 иллюстрирует пример транзакции для безопасной передачи компонентов времени выполнения между пользовательским устройством UE и поставщиком программного обеспечения в соответствии с одним вариантом осуществления изобретения.

Фиг.4 представляет собой вариант осуществления способа безопасного выполнения электронного модуля идентификации абонента (eSIM) в соответствии с изобретением.

Фиг.4А иллюстрирует вариант осуществления архитектуры самозагружаемой

операционной системы, карты eUICC и модулей eSIM в соответствии с изобретением.

Фиг.5 представляет собой логическую схему одного варианта осуществления обобщенного способа безопасной модификации и сохранения компонентов для использования с клиентами управления доступом.

Фиг.6 представляет собой логическую схему одного варианта осуществления обобщенного способа безопасного выполнения и сохранения компонентов для использования с клиентами управления доступом в соответствии с изобретением.

Фиг.7 представляет собой функциональную схему примерного устройства, предназначенного для реализации предлагаемых способов.

Осуществление изобретения

Далее приводятся ссылки на чертежи, на которых одинаковые ссылочные номера позиций относится к одинаковым элементам.

Обзор

В настоящем изобретении предлагаются в том числе безопасные (защищенные) способы и устройство, посредством которых пользовательское устройство и любая доверенная сторонняя структура могут взаимно верифицировать друг друга. Также предлагаются способ и устройство, которые позволяют любой сторонней структуре стать доверенной структурой даже после того, как пользовательское устройство было отправлено потребителю. Например, мобильное устройство (например, пользовательское устройство UE сети UMTS) может идентифицировать электронный модуль идентификации абонента (например, виртуальный или электронный модуль SIM, далее - модуль eSIM) стороннего поставщика и инициировать доверенную двустороннюю связь с целью приобретения, получения или обновления своего модуля eSIM. Таким же образом сторонний поставщик модуля eSIM может верифицировать, что пользовательское устройство UE является доверенным устройством, и безопасно закодировать свой модуль eSIM для передачи. Доверенная двусторонняя связь основана на уникальном ключе устройства и подтверждающем сертификате, при этом, как описано далее в настоящем документе, в одном примерном варианте осуществления ключ устройства основан на криптографии с использованием открытого/секретного ключа.

Различные аспекты настоящего изобретения направлены на обеспечение безопасного приема клиента управления доступом (полностью или частично). Ввиду важного характера контента управления доступом для операторов сети в существующих решениях используются форм-факторы физической карты. Однако в настоящем изобретении предлагается безопасная передача виртуальных или электронных клиентов управления доступом (например, модулей eSIM), благодаря чему устраняется необходимость использования физических карт и связанные с ними ограничения.

Кроме того, в отличие от существующих решений настоящее изобретение обеспечивает передачу контента клиента управления доступом без предварительно имеющегося клиента управления доступом, благодаря чему существенно повышается гибкость и удобство использования пользователем.

Еще в одном аспекте изобретения устройство (например, мобильное пользовательское устройство) может активировать и выполнять один из нескольких сохраненных клиентов управления доступом (например, модулей eSIM). В частности, при загрузке модуля eSIM операционной системе (OS) необходимо лишь загрузить перечень программного обеспечения, необходимого для текущей среды времени выполнения. Такой эффект изолированной среды («песочницы») обеспечивает возможность использования

нескольких модулей eSIM в одном и том же устройстве без нецелесообразного доступа к другим модулям eSIM.

Подробное описание примерных вариантов осуществления

Далее подробно описаны примерные варианты осуществления и аспекты настоящего изобретения. Несмотря на то что указанные варианты осуществления и аспекты главным образом рассмотрены в контексте модулей идентификации абонента (модулей SIM) сотовых сетей GSM, GPRS/EDGE или UMTS, специалистам в данной области техники должно быть понятно, что настоящее изобретение этим не ограничивается. Напротив, различные аспекты настоящего изобретения могут применяться в любой беспроводной сети (сотовой или другой), в которой требуется безопасная модификация, сохранение и выполнение структур или клиентов управления доступом.

Следует также понимать, что несмотря на то что в настоящем документе используется термин «модуль идентификации абонента» (например, модуль eSIM), данный термин не подразумевает и не требует обязательного (i) использования непосредственно абонентом (то есть настоящее изобретение может использоваться как абонентом, так и не абонентом), (ii) наличия отдельного человека (то есть настоящее изобретение может использоваться от лица группы людей, например семьи, нематериальной или воображаемой группы, такой как предприятие), (iii) какого-либо материального оборудования или аппаратного обеспечения «модуля».

Функционирование известного модуля идентификации абонента (модуля SIM)

В контексте сотовых сетей UMTS известного уровня техники пользовательское устройство (UE) включает мобильное устройство и универсальный модуль идентификации абонента (USIM, Universal Subscriber Identity Module). Модуль USIM представляет собой логическую программную структуру, хранящуюся в физической универсальной карте с интегральной схемой (UICC) и выполняемую с нее. В модуле USIM хранится различная информация, например информация абонента, а также ключи и алгоритмы, используемые для аутентификации у оператора сети с целью получения услуг беспроводной сети. Программное обеспечение модуля USIM основано на языке программирования Java Card™. Язык Java Card является разновидностью языка программирования Java™, модифицированного для «внедряемых» устройств типа карт (как, например, указанная выше карта UICC).

В целом карты UICC программируют модулем USIM до распространения среди абонентов, при этом предварительное программирование или персонализация индивидуальна для каждого оператора сети. Например, до развертывания модуль USIM связывают с международным идентификационным номером оборудования абонента (IMSI, International Mobile Subscriber Identify), уникальным идентификатором карты с интегральной схемой (ICC-ID, Integrated Circuit Card Identifier) и индивидуальным ключом аутентификации (K). Оператор сети хранит данную связь в регистре, содержащемся в центре аутентификации сети (AuC, Authentication Center). После персонализации карта UICC может быть распространена среди абонентов.

Далее со ссылкой на фиг.1 подробно описана одна примерная процедура аутентификации и согласования ключа (AKA, Authentication and Key Agreement) с использованием указанного выше модуля USIM из уровня техники. В обычных процедурах аутентификации пользовательское устройство UE получает идентификационный номер IMSI из модуля USIM. Пользовательское устройство UE передает идентификационный номер IMSI в обслуживающую сеть (SN, Serving Network) оператора сети или гостевой базовой сети. Обслуживающая сеть SN направляет запрос аутентификации в центр аутентификации AuC домашней сети (HN, Home Network).

Домашняя сеть HN сравнивает принятый идентификационный номер IMSI с регистром центра аутентификации AuC и получает соответствующий ключ K. Домашняя сеть HN формирует произвольное число (RAND) и подписывает его ключом K с использованием алгоритма для создания ожидаемого отклика (XRES). Домашняя сеть HN дополнительно формирует шифровальный ключ (CK, Cipher Key) и ключ целостности (IK, Integrity Key), предназначенные для использования в шифровании и защите целостности, а также аутентификационный маркер (AUTN, Authentication Token) с использованием различных алгоритмов. Домашняя сеть HN передает аутентификационный вектор, состоящий из произвольного числа RAND, отклика XRES, шифровального ключа CK и аутентификационного маркера AUTN, в обслуживающую сеть SN. Обслуживающая сеть SN сохраняет аутентификационный вектор только для использования в единовременном процессе аутентификации. Обслуживающая сеть SN передает произвольное число RAND и аутентификационный маркер AUTN в пользовательское устройство UE.

После приема пользовательским устройством UE произвольного числа RAND и аутентификационного маркера AUTN модуль USIM верифицирует достоверность аутентификационного маркера AUTN. В положительном случае пользовательское устройство UE использует принятое произвольное число RAND для вычисления своего собственного отклика (RES) с использованием сохраненного ключа K и того же самого алгоритма, посредством которого сформирован отклик XRES. Пользовательское устройство UE возвращает отклик RES в обслуживающую сеть SN. Обслуживающая сеть SN сравнивает отклик XRES с принятым откликом RES и, если они совпадают, обслуживающая сеть SN разрешает пользовательскому устройству UE пользоваться услугами беспроводной сети оператора.

Пример функционирования

Далее описаны различные аспекты настоящего изобретения со ссылкой на один пример реализации. В контексте примерного варианта осуществления настоящего изобретения вместо использования физической карты UICC, как в уровне техники, карту UICC эмулируют как виртуальную или электронную структуру, например как программное приложение, которую далее называют электронной универсальной картой с интегральной схемой (eUICC), которая содержится в безопасном элементе (например, безопасном микропроцессоре или устройстве хранения) в пользовательском устройстве UE. Карта eUICC выполнена с возможностью хранения и управления несколькими элементами модулей SIM, далее называемыми электронными модулями идентификации абонента (eSIM). Каждый модуль eSIM представляет собой программную эмуляцию типового модуля USIM и содержит аналогичные программные средства и связанные с ними пользовательские данные. Карта eUICC выбирает модуль eSIM на основании идентификатора ICC-ID модуля eSIM. После того как карта eUICC выбрала требуемый модуль (требуемые модули) eSIM, пользовательское устройство UE может инициировать процедуру аутентификации для получения услуг беспроводной сети от оператора сети, соответствующего модулю eSIM. Кроме того, каждое приложение модуля eSIM в целом охватывает клиенты управления доступом, такие как указанные выше модули USIM, CSIM, ISIM, SIM, RUIM и т.п. Понятно, что каждый модуль eSIM связан с учетной записью пользователя, и, таким образом, модуль eSIM может широко охватывать несколько клиентов управления доступом (например, модуль USIM и модуль SIM могут быть связаны с одной учетной записью модуля eSIM у пользователя).

Как указано выше, в описанной ранее процедуре модуля USIM из уровня техники используется предварительно розданный ключ для аутентификации в базовой сети

(например, указанной выше домашней сети (HN), обслуживающей сети (SN) и центре аутентификации (AuC) и т.п.). Соответственно процедура модуля USIM обязательно является закрытой системой для оператора сети, так как предварительно розданный ключ должен быть тщательно защищен. В настоящем изобретении, напротив, предлагаются безопасные способы, предназначенные для обеспечения взаимной доверительной связи между картой eUICC и какой-либо сторонней структурой, что позволяет любой сторонней структуре стать доверенной даже после развертывания пользовательского устройства.

Соответственно настоящее изобретение в некотором отношении предъявляет существенно более жесткие требования безопасности, но также позволяет добиться значительно большей гибкости. Кроме того, специалистам в данной области техники должно быть понятно, что несмотря на то что в различных аспектах настоящего изобретения могут использоваться виртуальные программные конструкции (например, карта eUICC, модуль eSIM), указанные преимущества не ограничиваются этими виртуальными вариантами осуществления. Напротив, раскрытые в настоящем документе принципы в равной степени применимы для безопасной модификации, сохранения и выполнения клиента управления доступом, заключенного в том числе в физических карточных носителях, специальном аппаратном обеспечении защиты и т.п.

Установление доверенной связи

На фиг.2 показан один примерный способ назначения пары ключей устройства программной структуре (например, карте eUICC, стороннему поставщику программного обеспечения, поставщику модулей SIM и т.п.). На шаге 202 программной структуре назначают криптографическую пару ключей открытый/секретный (например, алгоритма Rivest, Shamir и Adieman (RSA)) и сохраняют ее в физически защищенном безопасном элементе программной структуры, например карте eUICC в пользовательского устройства UE, безопасной базе данных у стороннего поставщика программного обеспечения. Например, карту eUICC программируют посредством доверенной структуры или, в альтернативном варианте, могут формировать внутри нее пару ключей открытый/секретный при начальном изготовлении/активации.

К сведению, пара ключей открытый/секретный основана на скрываемом секретном ключе и распространяемом открытом ключе. Схемы открытых/секретных ключей называются асимметричными, так как ключи, используемые для шифрования и дешифрования, различны, и, таким образом, шифрующая и дешифрующая стороны не имеют общего ключа. В симметричных схемах ключей, напротив, используется один и тот же ключ (или преобразуемые простым образом ключи) и для шифрования, и для дешифрования. Алгоритм RSA (Rivest, Shamir и Adieman) представляет собой один из типов криптографических алгоритмов пар ключей открытый/секретный, широко используемых в уровне техники, но следует понимать, что настоящее изобретение не ограничивается алгоритмом RSA.

Криптографические схемы открытый/секретный могут использоваться для шифрования сообщения и/или формирования подписей. В частности, сообщение может быть зашифровано секретным ключом и дешифровано открытым ключом, посредством чего можно гарантировать, что сообщение не изменено при передаче. Таким же образом, подпись, сформированная с использованием секретного ключа, может быть верифицирована открытым ключом, посредством чего можно гарантировать, что структура, формирующая подпись, является доверенной. В обоих случаях секретный ключ держится в тайне, а отрытый ключ распространяется свободно.

На шаге 204 для пары ключей открытый/секретный выдают подтверждающий

сертификат. Например, доверенная структура подтверждает аутентичность карты eUICC и секретность секретного ключа посредством выдачи подтверждающего сертификата для пары ключей карты eUICC. Эта пара ключей открытый/секретный теперь является парой ключей устройства для карты eUICC.

В одном варианте осуществления подтверждающий сертификат содержит набор данных, который может включать, среди прочего: (i) идентификационную информацию для удостоверяющего (сертифицирующего) органа, (и) идентификационную информацию для устройства, (iii) метаданные, описывающие алгоритмы сертификации, и/или (iv) соответствующие открытые ключи. Указанные компоненты дополнительно могут быть подписаны секретным ключом подтверждающей стороны. В одном варианте осуществления при нормальном функционировании эта цифровая подпись проверяется принимающей стороной для верификации того, что контент защищен и в него не были внесены посторонние изменения.

Так как пары ключей устройства являются асимметричными, открытые ключи могут распространяться без вреда для защиты и целостности секретных ключей. Соответственно ключ устройства и сертификат могут использоваться для защиты и верификации связи между не известными ранее друг другу сторонами (например, картой eUICC и другой стороной). Рассмотрим следующую примерную транзакцию для безопасной передачи компонентов времени выполнения между картой eUICC и поставщиком программного обеспечения (см. фиг.3).

На шаге 302, показанном на фиг.3, карта eUICC запрашивает модуль eSIM у стороннего поставщика модулей eSIM. Несмотря на то что в указанном примере описана безопасная передача приложения модуля eSIM, другие распространенные примеры приложений рабочей среды времени выполнения могут включать дополнения, полномасштабные операционные системы и т.п.

На шаге 304 сторонний поставщик модулей eSIM получает открытый ключ устройства, соответствующий карте eUICC, из подтверждающего сертификата, например подтверждающий сертификат может быть получен из базы данных, путем передачи запроса в карту eUICC и т.п. Следует отметить, что соответствующий секретный ключ карты eUICC в этом процессе никогда не раскрывается сторонним поставщикам модулей eSIM.

На шаге 305 сторонний поставщик модулей eSIM верифицирует подтверждающий сертификат. В одном примерном варианте осуществления подтверждающий сертификат уникальным образом подписан доверенной структурой (например, представитель компании Apple™). После того как сторонний поставщик модулей eSIM верифицировал подтверждающий сертификат, он может быть уверен в том, что карта eUICC является доверенной для доверенной структуры (например, Apple™), и, следовательно, является безопасной, защищенной.

На шаге 306 рабочая среда времени выполнения модуля eSIM шифруется и затем подписывается сторонним поставщиком программного обеспечения для конкретной карты eUICC, соответствующей пользовательскому устройству UE. В других вариантах осуществления рабочая среда времени выполнения модуля eSIM сначала подписывается, а затем шифруется. В одном примерном варианте поставщик использует свой собственный асимметричный ключ подписи и открытый/секретный ключ алгоритма RSA, а также цепь сертификатов для подписывания модуля eSIM, и использует краткосрочный или временный симметричный ключ для шифрования модуля eSIM. Данный временный симметричный ключ формируется случайным образом при подготовке пакета для карты eUICC.

На шаге 308 подписанная и зашифрованная рабочая среда модуля eSIM разбивается на несколько пакетов для передачи (например, по беспроводному интерфейсу и т.п.) сторонним поставщиком модулей eSIM. Например, подписанный и зашифрованный модуль eSIM разбивается на пакеты, соответствующие качеству канала связи (пакетная передача поддерживает различные требуемые схемы исправления ошибок, хорошо известные в данной области техники).

На шаге 310 краткосрочный симметричный ключ безопасным образом передается в карту eUICC, например, посредством его шифрования с помощью соответствующего открытого ключа карты eUICC. Сертификат поставщика может быть передан как открытый текст или, в альтернативном варианте, может быть зашифрован. В целом сертификат поставщика не зашифровывают для уменьшения вычислительной нагрузки на принимающей стороне (однако это не является требованием системы, и шифрование может использоваться либо во всех случаях, либо в альтернативном варианте может использоваться выборочно).

На шаге 312 карта eUICC верифицирует сертификат поставщика. Следует отметить, что успешная верификация сертификата поставщика с использованием открытого ключа подписи поставщика предоставляет карте eUICC доказательство того, что подпись не подделана.

В некоторых случаях сертификат поставщика может включать дополнительные подписи, выполненные внешней доверенной структурой (например, оператором сети мобильной связи и т.п.). Если сертификат поставщика действителен, то пользовательское устройство UE дешифрует краткосрочный симметричный ключ с использованием своего секретного ключа (секретного ключа карты eUICC). Успешное завершение вышеупомянутого обмена обеспечивает безопасность канала между картой eUICC и сторонней структурой и его шифрование канала с использованием общего краткосрочного симметричного ключа для последующей передачи данных.

Соответственно на шаге 314 карта eUICC может безопасным образом принять, восстановить и дешифровать множество зашифрованных пакетов. В этом конкретном примере карта eUICC загружает пакеты для модуля eSIM.

В одном варианте осуществления сертификат поставщика, ключ и зашифрованные пакеты передаются вместе. В альтернативных вариантах осуществления используются другие подходы, например передаются сертификат и ключ, и сначала устанавливается безопасное соединение, а затем инициируется передача зашифрованных пакетов по безопасному соединению.

В примерном варианте осуществления настоящего изобретения модуль eSIM рассматривается как отдельная от карты eUICC структура. Соответственно карта eUICC может установить безопасное соединение со сторонней структурой при отсутствии модуля eSIM и даже после развертывания пользовательского устройства. Указанный пример карты eUICC обеспечивает безопасную передачу модуля eSIM, что позволяет стороннему поставщику модулей eSIM напрямую распространять модули eSIM среди мобильных устройств, при этом зависимость от существующей процедуры SIM AKA, как в уровне техники, отсутствует.

Другими словами, устройство имеет ассиметричную пару ключей устройства, отдельную от симметричного ключа, связанного с любым отдельным модулем eSIM (и оператором сотовой сети, MNO, выдающим модули eSIM). Различие между модулем eSIM и картой eDICC имеет существенное влияние на сложность операционной системы устройства.

Выполнение безопасных сегментов

Как указано выше, существующие решения для физических карт UICC содержат одну структуру USIM, однако специалистам в данной области техники должно быть очевидно, что различные аспекты настоящего изобретения также подходят для сохранения и выполнения нескольких профилей клиента управления доступом. Соответственно в другом варианте осуществления настоящего изобретения карта eUICC должна определять достоверность как сети, так и модуля eSIM. Ввиду сложности указанных выше задач архитектуры модуля SIM уровня техники больше недостаточно для инициализации. Вместо этого в одном примерном варианте осуществления изобретения самозагружаемая операционная система (bootstrap operating system, bootstrap OS) загружает общую или резидентную операционную систему, общая операционная система загружает соответствующий модуль eSIM, и загруженный модуль eSIM может выполнять описанную выше процедуру аутентификации и согласования ключа (АКА).

В частности, самозагружаемая операционная система настоящего изобретения в одном варианте осуществления отвечает за криптографическую верификацию, дешифрование и загрузку общей операционной системы, а также всех дополнений, связанных с активируемым модулем eSIM. Самозагружаемая операционная система выполняется в виртуальной программной карте eUICC, следовательно, модуль eSIM и связанная операционная система выполняются в изолированной среде («песочнице») и могут осуществлять доступ только к соответствующим дополнениям, доступ к которым осуществляется посредством карты eUICC. Например, в одном примерном варианте осуществления карта eUICC активирует только те дополнения, которые используют ту же подписывающую сторону, что и модуль eSIM.

Далее со ссылкой на фиг.4 описан один примерный способ выполнения сегментирования модуля eSIM безопасным образом.

На шаге 402 карта eUICC запускает самозагружаемую операционную систему при перезапуске микросхемы. На шаге 404 самозагружаемая операционная система анализирует заданный список дополнений для рабочей среды времени выполнения. Например, самозагружаемая операционная система может идентифицировать сеть по умолчанию и связанные с ней дополнения. По меньшей мере одним из указанных дополнений является общая операционная система, а другие дополнения включают активный модуль eSIM и любые дополнительные дополнения, связанные с модулем eSIM.

На шаге 406 самозагружаемая операционная система верифицирует целостность дополнений, например, путем анализа сертификата или использования других средств. Например, в одном варианте осуществления доверенная структура (например, зарегистрированный представитель) может выдавать сертификаты или служить другим образом в качестве корневого источника подтверждения для цепочек подписей. Если дополнения должным образом подписаны, то самозагружаемая операционная система может выполнять их. Загружаются только верифицированные дополнения, соответствующие модулю eSIM (другие дополнения могут храниться, но не выполняются в «песочнице»).

На шаге 408 самозагружаемая операционная система запускает общую операционную систему. Общая операционная система предоставляет интерфейс между модулем eSIM и остальным аппаратным обеспечением. Общая операционная система в целом предоставляет входные и выходные функции, которые эмулируют карту UICC, характерную для конкретного модуля eSIM. В целом к этим функциям относятся такие функции как файловый ввод и вывод (10) и т.п.

Затем на шаге 410 общая операционная система может выполнять соответствующий

модуль eSIM.

На фиг.4A показана программная взаимосвязь 450 между самозагружаемой операционной системой 452, общей операционной системой 454 и модулями 456 eSIM. Следует отметить, что в примерном варианте осуществления (показанном на фиг.4 и 4A) различные профили модуля eSIM функционируют в своих собственных общих операционных системах. Благодаря разделению рабочих сред времени выполнения для разных профилей eSIM на отдельные изолированные среды («песочницы»), указанный выше вариант осуществления остается совместимым с традиционными архитектурами SIM и одновременно обладает преимуществами настоящего изобретения. В целом, путем обеспечения выполнения каждого модуля eSIM в своей собственной среде существующее программное обеспечение модуля SIM может быть непосредственно виртуализировано. Кроме того, изолированные среды («песочницы») гарантируют, что существование других модулей eSIM не вызовет негативных взаимодействий, что является требованием, необходимым для поддержки широкого круга сторонних поставщиков модулей eSIM (например, которые могут иметь проприетарные протоколы и возможности и т.п.).

Как указано выше, представленное выше описание основано главным образом на технологиях и свойствах сетях, основанных на модуле идентификации абонента. Соответственно далее приведено описание примерных вариантов осуществления обобщенных способов и устройства для реализации одного или нескольких аспектов настоящего изобретения.

Способы

Далее со ссылкой на фиг.5 описан один вариант осуществления обобщенного способа 500 для безопасной модификации и сохранения компонентов для использования с клиентами управления доступом.

На шаге 502 запрашивают или предлагают один или большее количество компонентов для использования с клиентом управления доступом. В одном примерном варианте осуществления указанные один или большее количество компонентов включают полностью или частично (i) общую операционную систему, (ii) по меньшей мере один модуль eSIM и/или (iii) одно или большее количество персонализирующих дополнений, связанных с модулем eSIM. В других технологических реализациях пакеты могут быть связаны с модулями идентификации абонента CDMA (CSIM), модулем идентификации мультимедийных служб протокола IP (ISIM), модулями идентификации абонента (SIM), удаляемыми модулями идентификации абонента (RUIM) и т.п. Специалистам в данной области техники, знакомым с настоящим описанием, должны быть очевидны множество комбинаций различных аналогичных структур, при этом модификации описанных в настоящем документе способов и устройств, предназначенных для реализации таких аналогичных структур и комбинаций, должны быть очевидны указанным специалистам, знакомым с настоящим описанием.

В одном варианте осуществления один или большее количество компонентов запрашиваются или загружаются устройством или абонентом, связанным с устройством, то есть пользователем/устройством, выдающим подтверждение связи или запрос. В альтернативных вариантах осуществления один или большее количество компонентов назначают или доставляют устройству, то есть без указанной выше связи или запроса, в соответствии с какими-либо другими критериями или схемой, например периодически, на основании возникновения какого-либо события и т.п. Информация о существовании одного или большего количества компонентов может сообщаться или другим образом передаваться или сохраняться в хранилище, к которому может предоставляться доступ

и в котором может осуществляться поиск.

В других вариантах осуществления один или большее количество компонентов запрашиваются или другим образом активируются посредством одного или большего количества контекстуальных событий, например при входе устройства в заданную зону, превышении заданных объемов использования и т.п.

Запрос или предложение может включать подпись или сертификат, сформированный доверенной стороной. В других альтернативных реализациях запрос или предложение содержат криптографическую информацию-вызов. В других вариантах осуществления запрос или предложение включает средство для определения подлинности (например, аутентификация по паролю с использованием пользовательского интерфейса и т.п.).

Запрос или предложение также может включать транзакционный ключ. В одном таком варианте транзакционный ключ является кратковременным ключом. При этом также могут применяться другие постоянные транзакционные ключи, например ключ может быть одним и тем же для нескольких сеансов транзакций, нескольких пользователей и т.п. В других вариантах транзакционный ключ представляет собой симметричный ключ или, в альтернативном варианте, асимметричный ключ.

На шаге 504 запрос или предложение верифицируют для определения аутентичности (подлинности). В одном варианте осуществления подпись или сертификат, сформированный доверенной стороной, проверяют на достоверность. В некоторых случаях это может потребовать внешней связи с доверенной стороной. В альтернативном варианте достоверность подписи или сертификата может быть самоочевидна или может определяться другим образом верифицирующей стороной без обращения к доверенной стороне. Другие схемы могут быть основаны на данных, поступающих от абонента, например вводе имени пользователя и пароля или простых схемах подтверждения и т.п.

Успешная верификация также может требовать одного или большего числа обменов вызов-ответ. В некоторых вариантах верификация может быть однонаправленной (например, верифицируется только одна из сторон транзакции) или двунаправленной (например, должны быть успешно верифицированы обе стороны транзакции). В других схемах верификацию осуществляют за пределами полосы связи (например, посредством другого канала связи) или с помощью абонента и т.п.

Положительные результаты верификации приводят к достижению соглашения по одному или большему количеству параметров, необходимых для безопасной транзакции. Например, в одном варианте осуществления определяются один или большее количество транзакционных ключей. В некоторых вариантах транзакционный ключ формируется после верификации. В альтернативных вариантах транзакционный ключ предлагается или формируется до верификации и используется после верификации при определенных условиях.

Затем на шаге 506 устройство принимает один или большее количество пакетов, связанных с клиентом управления доступом. Пакеты могут быть дополнительно зашифрованы с использованием транзакционного ключа для обеспечения безопасной передачи. В одном варианте пакеты шифруются асимметричным образом, то есть пакеты шифруются с использованием открытого ключа. В других вариантах пакеты шифруются симметричным образом с использованием предварительно согласованного общего ключа. В альтернативных вариантах пакеты подписываются подписью, обеспечивающей возможность идентификации. В настоящем изобретении могут использоваться множество других решений для передачи пакетов с возможностью верификации, известных в данной области техники.

На шаге 508 устройство восстанавливает пакеты и дешифрует один или большее количество компонентов. В одном примерном варианте осуществления один или большее количество компонентов связаны с соответствующей общей операционной системой. Например, как описано выше, дополнения могут включать по меньшей мере один модуль eSIM и/или одно или большее количество персонализирующих дополнений, связанных с модулем eSIM, как описано выше. По завершении шага 508 один или большее количество компонентов успешно и безопасно переданы в целевое устройство.

Далее со ссылкой на фиг.6 описан примерный вариант осуществления обобщенного способа 600 для безопасного выполнения компонентов для использования с клиентами управления доступом.

На шаге 602 идентифицируется клиент управления доступом и одно или большее количество соответствующих дополнений. В одном примерном варианте осуществления клиент управления доступом и одно или большее количество соответствующих дополнений выбираются операционной системой. В одной реализации операционная система дополнительно загружается из простой самозагружаемой операционной системы.

В одной конфигурации самозагружаемая операционная система обеспечивает несколько безопасных сегментов, при этом каждый сегмент отличается от других сегментов, а программное обеспечение, выполняемое из сегмента памяти, не может иметь доступ к другим несвязанным сегментам, и другие несвязанные сегменты не имеют доступа к нему. Например, одно примерное устройство выполняет простую самозагружаемую операционную систему, которая загружает и выполняет общую операционную систему и связанные с ней модули eSIM, а также дополнения в одном сегменте изолированной среды («песочницы»).

В различных вариантах осуществления настоящего изобретения все доступные компоненты и дополнения разделены в соответствии с одной или большим количеством категорий. В одном таком варианте компоненты и дополнения связаны в соответствии с общей подписывающей стороной или доверенным источником. Например, в одном случае простая самозагружаемая операционная система может разрешать для выполнения лишь общую операционную систему и модули eSIM, подписанные одним и тем же поставщиком модулей eSIM. В других вариантах компоненты и дополнения могут быть сопоставлены в соответствии с выбором пользователя или различными уровнями доверия. Например, различные компоненты могут быть взяты из разных взаимодействующих структур (например, доверенного поставщика модулей eSIM и персонализации доверенной сети и т.п.).

На шаге 604 способа 600 клиент управления доступом и соответствующие дополнения верифицируются для функционирования. В одном варианте осуществления клиент управления доступом и соответствующие дополнения проверяются на целостность, то есть проверяют, не были ли в них внесены неправомерные изменения или не изменены ли они другим образом. К распространенным способам таких проверок целостности относятся контрольные суммы, криптографические хэш-функции или вычеты и т.п. Другие решения для верификации аутентичности дополнений могут включать верификацию сертификата, верификацию состояния и т.п.

На шаге 606 выполняется верифицированный клиент управления доступом. При успешной загрузке и выполнении клиент управления доступом выполняет первоначальные процедуры управления доступом для соответствующей сети. Например, верифицированный модуль eSIM может выполнять процедуру аутентификации и согласования ключа.

Примерное мобильное устройство

Далее со ссылкой на фиг.7 описано примерное устройство 700, предназначенное для реализации способов в соответствии с настоящим изобретением.

Примерное пользовательское устройство UE, показанное на фиг.7, представляет собой беспроводное устройство с вычислительной подсистемой 702, например цифровым сигнальным процессором, микропроцессором, программируемой логической матрицей или множеством вычислительных компонентов, установленных на одной или нескольких подложках. Вычислительная подсистема также может содержать внутреннюю кэш-память. Вычислительная подсистема соединена с подсистемой 704 памяти, содержащей память, которая может включать, например, компоненты SRAM, флеш-память и SDRAM. Подсистема памяти может реализовывать одно или большее количество аппаратных средств с прямым доступом к памяти для ускорения доступа к данным, что хорошо известно в данной области техники. Подсистема памяти содержит выполняемые компьютером инструкции, которые выполняются вычислительной подсистемой.

В одном примерном варианте осуществления настоящего изобретения устройство может содержать один или большее количество беспроводных интерфейсов (706), выполненных с возможностью подключения к одной или большему количеству беспроводных сетей. Несколько беспроводных интерфейсов могут поддерживать разные технологии радиосвязи, например GSM, CDMA, UMTS, LTE/LTE-A, WiMAX, WLAN, Bluetooth и т.п., посредством реализации соответствующих антенной и модемной подсистем.

Подсистема 708 пользовательского интерфейса включает любое количество известных средств ввода/вывода (I/O), включая среди прочего клавиатуру, сенсорный экран (например, сенсорный интерфейс «multi-touch»), жидкокристаллический экран, подсветку, громкоговоритель и/или микрофон. Однако понятно, что в определенных условиях один или большее количество указанных компонентов могут быть опущены. Например, в вариантах осуществления с клиентом на карте PCMCIA может отсутствовать пользовательский интерфейс (так как в них может использоваться пользовательский интерфейс хост-устройства, с которым эти карты физически и/или электрически соединены).

В представленном варианте осуществления устройство содержит безопасный элемент 710, который содержит и эксплуатирует приложение карты UICC. Карта eUICC реализована с возможностью сохранения и осуществления доступа к множеству клиентов управления доступом, предназначенных для аутентификации у оператора сети. К безопасному элементу может осуществлять доступ подсистема памяти по запросу вычислительной подсистемы.

В одном примерном варианте осуществления безопасный элемент содержит по меньшей мере сегментируемую память, причем сегментируемая память может содержать один или большее количество клиентов управления доступом и соответствующих дополнений. Каждый сегмент отличается от других сегментов, а программное обеспечение, выполняемое из сегмента памяти, не может иметь доступ к другим несвязанным сегментам, и другие несвязанные сегменты не имеют доступа к нему.

Безопасный элемент также может содержать так называемый безопасный микропроцессор (SM), хорошо известный в области обеспечения безопасности.

Кроме того, различные реализации примерного варианта осуществления включают инструкции, которые при выполнении запускают простую самозагружаемую операционную систему. Самозагружаемая операционная система дополнительно обеспечивает возможность выбора по меньшей мере одного сегмента из безопасного

элемента и загрузки соответствующего клиента управления доступом, загружаемого с него. В различных реализациях клиенты управления доступом могут быть дополнительно снабжены одним или большим количеством сертификатов, связанных с доверенной подписывающей стороной. Самозагружаемая операционная система может верифицировать сертификаты до выполнения клиента управления доступом.

Кроме того, в одном варианте осуществления безопасный элемент поддерживает перечень или спецификацию хранящихся клиентов управления доступом. Указанная спецификация может включать информацию о текущем состоянии хранящихся клиентов управления доступом, при этом такая информация может включать информацию о доступности, полноте, действительности, возникавших ранее ошибках и т.п. Спецификация может быть дополнительно связана или соединена с пользовательским интерфейсом с целью обеспечения выбора пользователем доступного клиента управления доступом.

Как показано на фиг.7, безопасный элемент 710 может принимать и сохранять компоненты, предназначенные для использования с одним или большим количеством клиентов управления доступом для аутентификации у оператора сети. В одном примерном варианте осуществления безопасный элемент имеет соответствующий ключ устройства и подтверждающий сертификат. Данный ключ устройства используется для защиты и верификации связи между не известными ранее друг другу сторонами (например, пользовательским устройством UE и другой стороной).

В одном таком варианте ключ устройства представляет собой секретный ключ асимметричной пары ключей открытый/секретный. Дополняющий открытый ключ может свободно распространяться без негативного влияния на целостность секретных ключей. Например, устройству может назначаться (или устройство может само формировать) открытый/секретный ключ алгоритма RSA, при этом открытый ключ становится доступен для связи после развертывания.

Кроме того, в некоторых вариантах подтверждающий сертификат представляет собой уникальным образом подписанную цифровую подпись, соответствующую доверенной структуре. В одном примерном варианте подтверждающий сертификат верифицируется сторонними структурами и является доказательством целостности примерного устройства.

Несмотря на то что указанные выше способы и устройство для программирования безопасного элемента описаны со ссылкой на пару ключей алгоритма RSA, специалистам в данной области техники должно быть очевидно, что также могут использоваться другие схемы аутентификации. Например, в других вариантах ключ устройства может представлять собой общий ключ, при этом распространение общего ключа тщательно защищено. Другие варианты осуществления могут быть основаны на сертификатах, а не на обмене криптографическими ключами.

Понятно, что несмотря на то что определенные аспекты изобретения описаны со ссылкой на конкретный порядок шагов способа, это описание является всего лишь обобщенным примером реализации способа, и в соответствии с требованиями конкретной задачи данный порядок может быть изменен. В определенных условиях некоторые шаги могут оказаться ненужными или опциональными. Кроме того, некоторые шаги или функции могут быть добавлены к описанным вариантам осуществления, или может быть изменен порядок осуществления двух или более шагов. Все подобные изменения считаются входящими в описанное предлагаемое изобретение.

Несмотря на то что в приведенном выше подробном описании показаны, раскрыты и выделены новые признаки изобретения в различных вариантах осуществления,

понятно, что специалистами в данной области техники без отклонения от объема изобретения могут быть выполнены различные исключения, подстановки и изменения в предлагаемом устройстве или способе. Приведенное выше описание соответствует наилучшему варианту осуществления изобретения. Данное описание не является ограничительным и должно рассматриваться как иллюстрация общих принципов изобретения. Объем охраны изобретения должен определяться по формуле изобретения.

Формула изобретения

1. Беспроводное устройство связи, содержащее

один или большее количество интерфейсов беспроводной связи, обеспечивающих возможность осуществления связи с по меньшей мере одной сетью;

безопасный элемент, выполненный с возможностью хранения клиента управления доступом;

интерфейс к безопасному элементу, который связан с криптографическим ключом и связанным с ним первым сертификатом;

вычислительное устройство и

устройство хранения, соединенное с возможностью обмена данными с вычислительным устройством и содержащее выполняемые компьютером инструкции, при этом выполняемые компьютером инструкции при их выполнении вычислительным устройством обеспечивают выполнение вычислительным устройством следующих действий:

посредством интерфейса передают запрос одного или большего количества компонентов для клиента управления доступом, относящегося к по меньшей мере одной сети;

принимают один или большее количество запрошенных компонентов и второй сертификат;

верифицируют второй сертификат и

в ответ на успешную верификацию второго сертификата сохраняют клиент управления доступом в безопасном элементе, причем клиент управления доступом сохраняют в индивидуальном сегменте из числа множества сегментов, из которых состоит безопасный элемент, и последующие модификации сохраненного клиента управления доступом могут быть выполнены только с использованием второго сертификата.

2. Устройство по п.1, отличающееся тем, что клиент управления доступом включает один или большее количество электронных модулей идентификации абонента (eSIM); безопасный элемент включает электронную универсальную карту с интегральной схемой (eUICC), а каждый из указанных одного или большего количества модулей eSIM связан с международным идентификационным номером оборудования абонента (IMSI); и каждый из модулей eSIM дополнительно обеспечивает возможность установления безопасного соединения с сотовой сетью на основании, по меньшей мере частично, процедуры авторизации и согласования ключа (АКА).

3. Устройство по п.2, отличающееся тем, что указанная по меньшей мере одна сеть включает сеть глобального стандарта мобильной связи (GSM).

4. Устройство по п.2, отличающееся тем, что указанная по меньшей мере одна сеть включает сеть универсальной системы мобильной связи (UTMS).

5. Устройство по п.2, отличающееся тем, что указанная по меньшей мере одна сеть включает сеть с множественным доступом с кодовым разделением 2000 (CDMA 2000).

6. Устройство по п.1, отличающееся тем, что указанный запрос включает первый

сертификат.

7. Устройство по п.6, отличающееся тем, что криптографический ключ уникальным образом связан с первым сертификатом.

8. Устройство по п.1, отличающееся тем, что криптографический ключ имеет асимметричный дополняющий ключ, который может распространяться открыто.

9. Устройство по п.8, отличающееся тем, что указанный асимметричный дополняющий ключ обеспечивает безопасную передачу в беспроводное устройство связи.

10. Устройство по п.1, отличающееся тем, что указанные один или большее количество компонентов включают клиент управления доступом, зашифрованный посредством сеансового ключа, а первый и второй сертификаты содержат соответственно первый и второй подтверждающий сертификаты.

11.Устройство по п.10, отличающееся тем, что указанный сеансовый ключ сформирован случайным образом.

12. Способ запроса пользовательского клиента управления доступом для использования с беспроводной сетью, включающий:

запрос пользовательского клиента управления доступом из беспроводной сети, при этом запрос связан с первым подтверждающим сертификатом;

прием пользовательского клиента управления доступом и второго подтверждающего сертификата, при этом первый и второй подтверждающий сертификаты выданы доверенной структурой; и

сохранение пользовательского клиента управления доступом в безопасном элементе, если второй подтверждающий сертификат действителен; причем пользовательский клиент управления доступом сохраняют в индивидуальном сегменте из числа множества сегментов, из которых состоит безопасный элемент, и последующие модификации сохраненного пользовательского клиента управления доступом могут быть выполнены только с использованием второго подтверждающего сертификата; а

доступ к беспроводной сети ограничен (i) доступом посредством пользовательского клиента управления доступом и (ii) запросами пользовательских клиентов управления доступом.

13. Способ по п.12, отличающийся тем, что пользовательский клиент управления доступом включает электронный модуль идентификации абонента (eSIM).

14. Способ по п.12, отличающийся тем, что первый и второй подтверждающий сертификаты уникальным образом связаны с первой и второй криптографическими парами ключей соответственно.

15. Способ по п.14, отличающийся тем, что первая и вторая криптографические пары ключей содержат асимметричные пары ключей.

16. Способ по п.12, отличающийся тем, что пользовательский клиент управления доступом зашифрован посредством сеансового ключа.

17. Способ выполнения клиента управления доступом, включающий: выполнение самозагружаемой операционной системы, которая выбирает безопасный сегмент, связанный с клиентом управления доступом, причем клиент управления доступом обладает возможностью аутентификации в сети;

верификацию безопасного сегмента, включающего общую операционную систему и клиент управления доступом; и

выполнение общей операционной системы, которая загружает один клиент управления доступом.

18. Способ по п.17, отличающийся тем, что клиент управления доступом включает

электронный модуль идентификации абонента (eSIM).

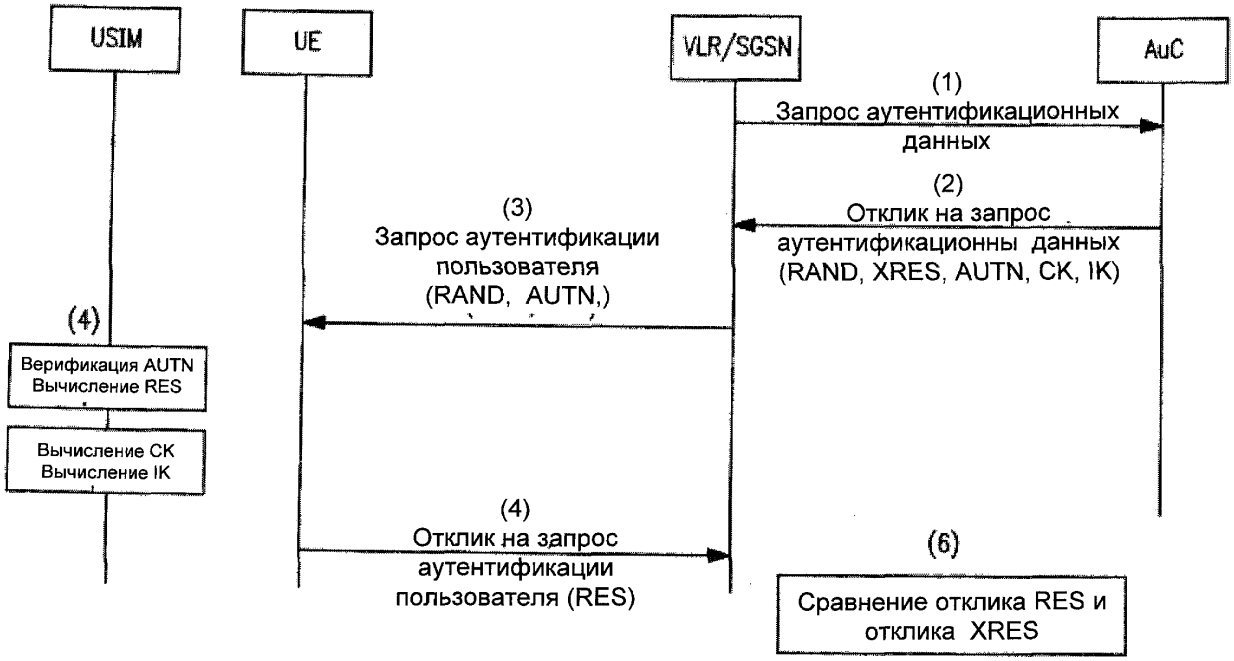
19. Способ по п.17, отличающийся тем, что шаг выбора включает идентификацию сети по умолчанию.

20. Способ по п.19, отличающийся тем, что верификация включает проверку сертификата, связанного с безопасным сегментом.

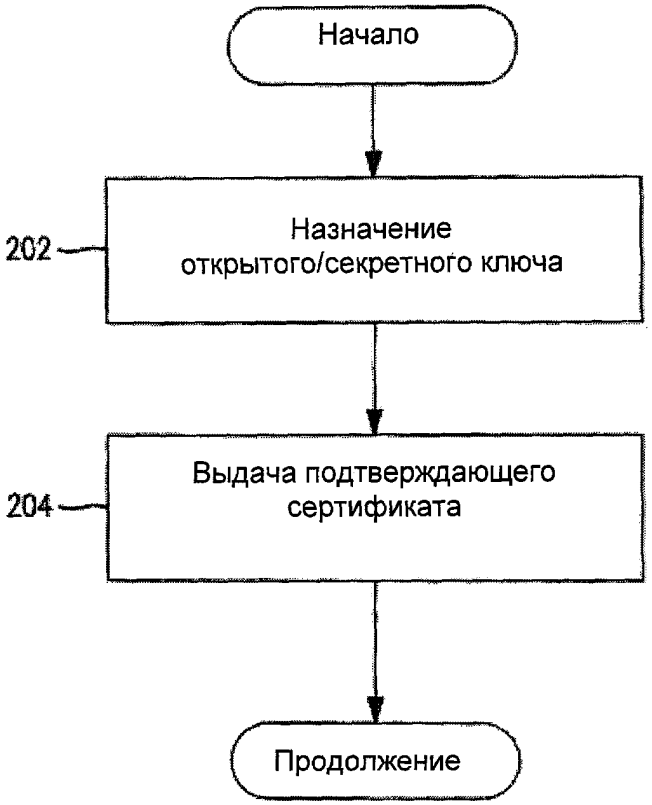
21. Способ по п.20, отличающийся тем, что безопасный сегмент включает одно или большее количество активных дополнений, каждое из которых связано с сертификатом.

22. Способ по п.17, отличающийся тем, что шаг выбора включает выбор безопасного сегмента из множества безопасных сегментов, каждый из которых связан лишь с одним клиентом управления доступом.

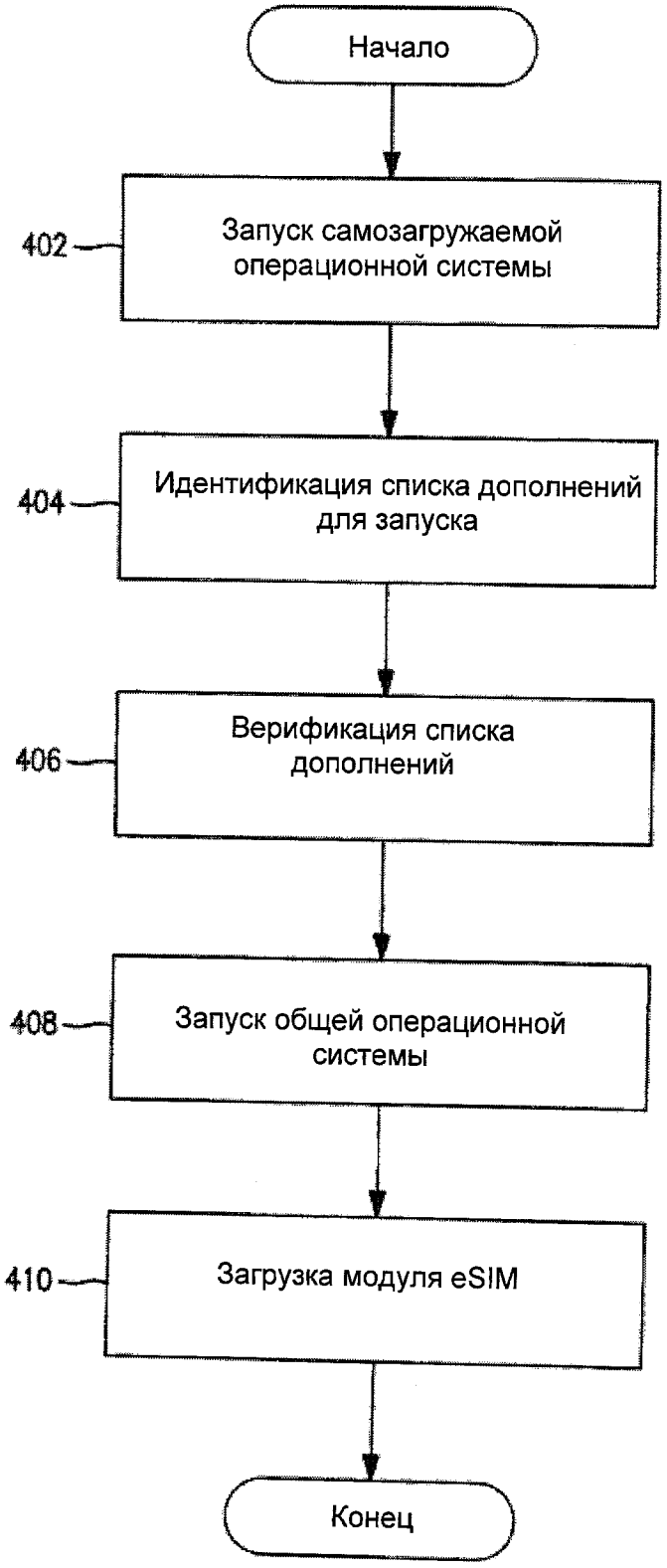
Процесс аутентификации и согласования ключа



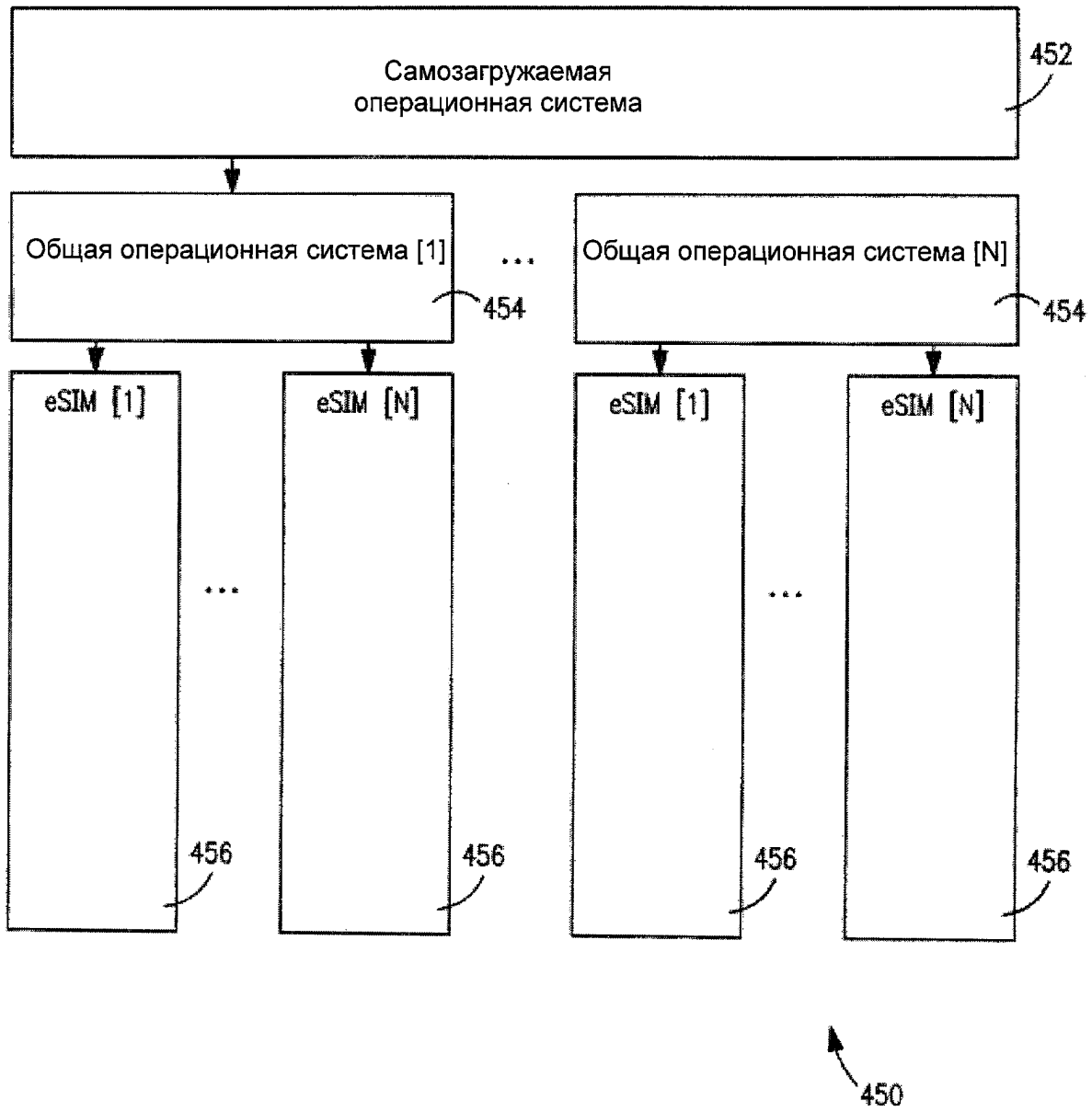
ФИГ.1



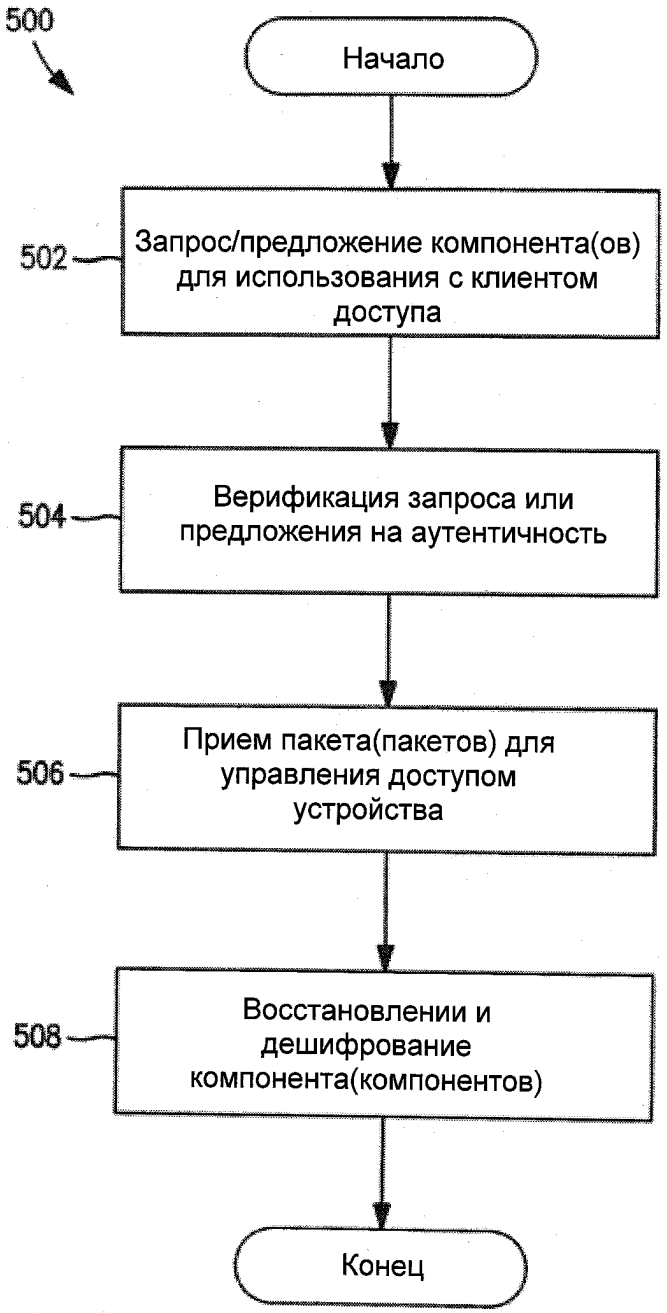
ФИГ.2


Начало
402
Запуск самозагружаемой операционной системы
404
Идентификация списка дополнений для запуска
406
Верификация списка дополнений
408
Запуск общей операционной системы
410
Загрузка модуля eSIM
Конец

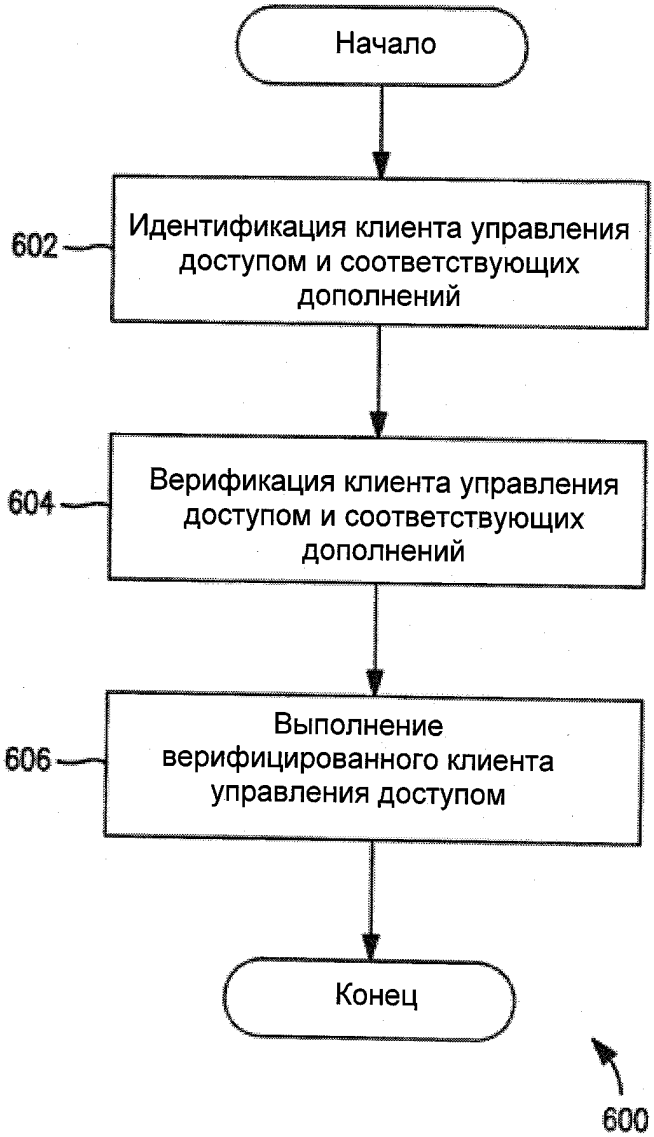
ФИГ.4


Самозагружаемая операционная система
452
Общая операционная система [1]
454
Общая операционная система [N]
454
eSIM [1]
eSIM [N]
eSIM [1]
eSIM [N]
456
456
456
456
450

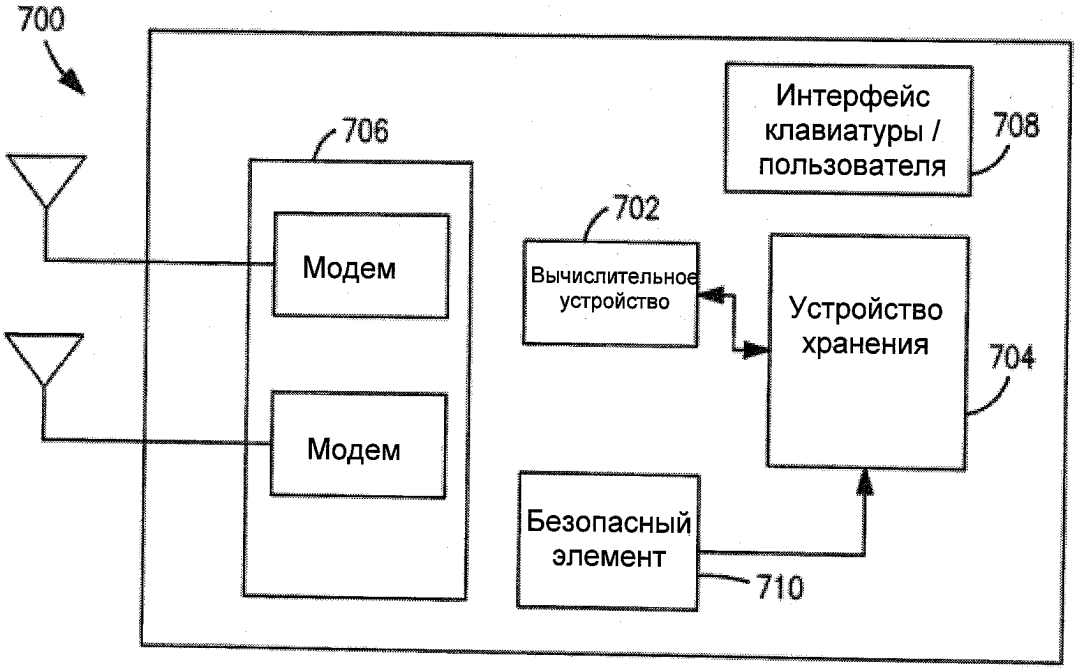
ФИГ.4А


500
Начало
502
Запрос/предложение компонента(ов) для использования с клиентом доступа
504
Верификация запроса или предложения на аутентичность
506
Прием пакета(пакетов) для управления доступом устройства
508
Восстановлении и дешифрование компонента(компонентов)
Конец

ФИГ.5


Начало
602
Идентификация клиента управления доступом и соответствующих дополнений
604
Верификация клиента управления доступом и соответствующих дополнений
606
Выполнение верифицированного клиента управления доступом
Конец
600

ФИГ.6


700
706
Модем
Модем
Интерфейс клавиатуры / пользователя
708
702
Вычислительное устройство
Устройство хранения
704
Безопасный элемент
710

ФИГ.7