РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 411 670** (13) **C2**

(51) МПК
H04L 9/08 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2007102215/08, 24.06.2005**

(24) Дата начала отсчета срока действия патента:
24.06.2005

Приоритет(ы):
(30) Конвенционный приоритет:
25.06.2004 NO 20042691

(43) Дата публикации заявки: **27.07.2008** Бюл. № 21

(45) Опубликовано: **10.02.2011** Бюл. № **4**

(56) Список документов, цитированных в отчете о поиске: **WO 00/39958 A1, 06.07.2000. WO 03/093923 A2, 13.11.2003. WO 02/50643 A1, 27.06.2002. RU 2188514 C2, 27.08.2002. RU 93033427 A, 20.12.1995.**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **25.01.2007**

(86) Заявка PCT:
NO 2005/000230 (24.06.2005)

(87) Публикация заявки PCT:
WO 2006/001710 (05.01.2006)

Адрес для переписки:
191186, Санкт-Петербург, а/я 230, "АРС-ПАТЕНТ", пат.пов. М.В.Хмаре, рег. № 771

(72) Автор(ы):
СКОРВЕ Эйгил Тапио (NO),
ХЕНРИКСВЕЕН Мадс Эгил (NO),
ХАГЕН Йон (NO),
ЛИНДСТЁЛ Гуннар (NO),
ИМСДАЛЕН Толлеф (NO),
ЛИСНЕ Эдвард (NO),
КОММИСРУД Рагнхилд (NO)

(73) Патентообладатель(и):
БАЙПАСС АС (NO)

(54) СПОСОБ СОЗДАНИЯ И ПРОВЕРКИ ПОДЛИННОСТИ ЭЛЕКТРОННОЙ ПОДПИСИ

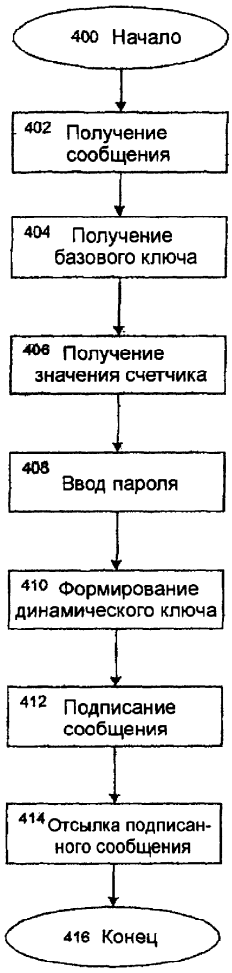
(57) Реферат:

Изобретение относится к защите данных и передаче данных в системах мобильной связи. Техническим результатом является устранение зависимости от оператора и повышение надежности защиты от злонамеренных атак или попыток мошеннического использования. Способ включает в себя этапы извлечения базового ключа из области памяти в терминале мобильной связи, осуществления ввода пользователем регистрационных данных, формирования динамического ключа на основе базового ключа и регистрационных данных; причем способ дополнительно включает в себя этапы получения электронного сообщения и формирования электронной подписи с использованием сгенерированного динамического ключа, причем этап извлечения базового ключа включает в себя получение базового ключа из области памяти, содержащей участок кода терминального приложения, загруженного на терминал мобильной связи, причем, по меньшей мере, базовый ключ сохранен в указанном участке кода в скрытом виде, при этом базовый ключ скрыт в коде таким образом, что его

RU 2411670 C2

RU 2411670 C2

невозможно прочитать напрямую или извлечь из кода. 3 н. и 5 з.п. ф-лы, 7 ил.



ФИГ. 4

RU 2411670 C2

RU 2411670 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 411 670** (13) **C2**

(51) Int. Cl.
H04L 9/08 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2007102215/08, 24.06.2005**

(24) Effective date for property rights:
24.06.2005

Priority:
(30) Priority:
25.06.2004 NO 20042691

(43) Application published: **27.07.2008** Bull. 21

(45) Date of publication: **10.02.2011 Bull. 4**

(85) Commencement of national phase: **25.01.2007**

(86) PCT application:
NO 2005/000230 (24.06.2005)

(87) PCT publication:
WO 2006/001710 (05.01.2006)

Mail address:
191186, Sankt-Peterburg, a/ja 230, "ARS-PATENT", pat.pov. M.V.Khmare, reg. № 771

(72) Inventor(s):
SKORVE Ehjgil Tapio (NO),
KhENRIKSVEEN Mads Ehgil (NO),
KhAGEN Jon (NO),
LINDSTEL Gunnar (NO),
IMSDALEN Tollef (NO),
LISNE Ehdvard (NO),
KOMMISRUD Ragnkhild (NO)

(73) Proprietor(s):
BAJPASS AS (NO)

RU 2411670 C2

(54) METHOD TO CREATE AND VERIFY AUTHENTICITY OF ELECTRONIC SIGNATURE

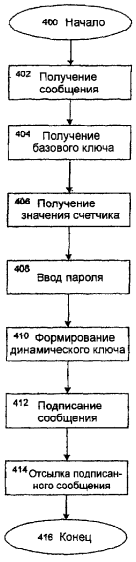
(57) Abstract:

FIELD: information technologies.

SUBSTANCE: method includes stages of basic key extraction from area of memory in terminal of mobile communication, user realising input of registration data, formation of dynamic key on the basis of basic key and registration data; besides, method additionally includes stages to produce electronic message, and formation of electronic signature using generated dynamic key, besides, stage of basic key extraction includes getting basic key from area of memory, containing section of code of terminal application, downloaded to terminal of mobile communication, besides, at least basic key is stored in specified section of code in hidden type. At the same time basic key is hidden in code so that it is not possible to read it directly or extract from code.

EFFECT: elimination of dependence on operator and improved reliability of protection against malicious attacks or attempts of fraudulent use.

8 cl, 7 dwg



ФИГ. 4

RU 2411670 C2

Область техники, к которой относится изобретение

Настоящее изобретение относится к общей области защиты данных и передачи данных в системах мобильной связи.

Более конкретно, изобретение касается способа, компьютерной программы и терминала мобильной связи для создания электронной подписи, обрабатываемой обрабатывающим модулем терминала мобильной связи. Изобретение также охватывает способ, компьютерную программу и сервер проверки для проверки электронной подписи.

Уровень техники

Вследствие общего развития технологий цифровой связи все большее количество типов обмена информацией и транзакций осуществляют в цифровой форме. В частности, распространение систем мобильной связи привело к использованию терминалов или портативных аппаратов мобильной связи, например телефонных аппаратов или персональных информационных систем (PDA), в различных формах электронной торговли и службах платежей с использованием мобильной связи.

При осуществлении таких служб существенным фактором является безопасность транзакций. Особенно важным является обеспечение надежной, эффективной и простой аутентификации личности пользователя терминала мобильной связи.

Простейшие технологии аутентификации, основанные на использовании имен пользователей и паролей, обладают рядом недостатков. В их число входит противоречие между необходимостью использования длинного и неповторимого пароля для обеспечения безопасности и желанием использования короткого и легко запоминающегося пароля для удобства пользователя. Пересылка паролей через открытые сети может привести к снижению защищенности системы.

В настоящее время операторы мобильной связи обладают широкими возможностями контроля инфраструктур каналов мобильной связи и, следовательно, услуг, предоставляемых с использованием таких каналов. В связи с этим ранее были описаны технологии аутентификации, основанные на использовании модулей идентификации абонентов (SIM, Subscriber Identity Module) терминалов мобильной связи.

Одна из общепризнанных известных технологий известна под названием «жесткой аутентификации». Данная технология основана на привязке электронного идентификатора к ключу шифрования, который сохраняют так, чтобы исключить доступ к нему лиц, не имеющих на это права, в частности, в электронной смарт-карте. Все операции, в которых требуется использование ключа, могут осуществляться внутри процессора, установленного на смарт-карте.

Известны варианты осуществления жесткой аутентификации, в которых SIM-карта терминала мобильной связи также представляет собой смарт-карту, содержащую ключ шифрования. Однако в этом случае оператор терминала мобильной связи, который является собственником смарт-карты, обладает возможностями полного управления ключом и операциями аутентификации, в которых используется данный ключ, т.к. модуль хранения ключа, предусмотренный в SIM-карте, недоступен независимому поставщику услуг. Поэтому решения такого рода не являются независимыми от оператора.

Обычные элементы памяти в терминале мобильной связи доступны независимому поставщику услуг и, следовательно, в принципе позволяют осуществлять независимые от оператора технологии аутентификации. Однако такие элементы памяти непригодны для хранения ключей, т.к. содержимое элементов памяти также

легкодоступно посторонним лицам.

В патентной публикации US 6529886 предлагается независимый от оператора процесс аутентификации, в котором основное значение придают обеспечению анонимности для посторонних лиц.

В данной публикации описаны: (1) использование счетчика со стороны клиента, (2) расхождение между клиентским ключом и главным ключом и (3) протокол однонаправленной аутентификации от клиента к серверу.

Настоящее изобретение отличается от представленного в данной публикации, в частности, тем, что предполагает генерирование динамических ключей с использованием главного ключа, счетчика и регистрационных данных, например, пароля или PIN-кода, что исключает необходимость сохранения динамического ключа в памяти мобильного телефона.

В патентной публикации US 2002/0099940 предлагается решение, в соответствии с которым пользователь устанавливает сетевое соединение с сервером аутентификации, который получает аутентификационную информацию в форме пароля. Затем в мобильное клиентское приложение загружают универсальную (независимую от технологической платформы) программу в форме прикладной программы на языке Java. Программа проходит идентификацию на сервере и устанавливает защищенное соединение.

Данная патентная публикация в основном рассматривает вопросы установления защищенного соединения и не может считаться относящейся к процессу создания подписей для сообщений. Данный документ не описывает процесса генерирования ключей, подобного используемому в настоящем изобретении.

Раскрытие изобретения

В соответствии с настоящим изобретением предлагается способ генерирования электронной подписи, осуществляемый модулем процессора терминала мобильной связи. Изобретение дополнительно охватывает способ проверки электронной подписи.

Одна из задач, на решение которой направлено изобретение, заключается в предложении способа, явно независимого от оператора.

Другая задача, на решение которой направлено изобретение, заключается в предложении способа вышеуказанного типа, обеспечивающего достаточно надежную защиту от злонамеренных атак или попыток мошеннического использования.

В соответствии с настоящим изобретением предлагается способ создания электронной подписи, описанный ниже в п.1 формулы изобретения, соответствующая компьютерная программа, описанная ниже в п.10 формулы изобретения, и соответствующий терминал мобильной связи, описанный ниже в п.14 формулы изобретения.

Кроме того, в соответствии с настоящим изобретением предлагается способ проверки подписи, описанный ниже в п.11 формулы изобретения, соответствующая компьютерная программа, описанная ниже в п.13 формулы изобретения, и соответствующий сервер проверки, описанный ниже в п.15 формулы изобретения.

Оптимальные варианты осуществления изобретения описаны в зависимых пунктах формулы изобретения.

В соответствии с изобретением гарантируется лишь временное использование динамического ключа в процессе формирования подписи. Поэтому динамический ключ не сохраняют. Кроме того, исключается сохранение в терминале мобильной связи или передача по каналам связи регистрационных данных пользователя, например пароля. Это способствует повышению безопасности.

Настоящее изобретение может быть использовано при применении таких терминальных приложений как программные средства идентификации или аутентификации пользователей, например, при предоставлении услуг заказов и/или платежей с использованием мобильной связи. При этом аутентификация не требует доступа к ключам или другим данным, сохраненным на SIM-карте, или использования других функций SIM-карты. Эти особенности настоящего изобретения обеспечивают независимость от оператора.

Краткое описание чертежей

Прилагаемые чертежи иллюстрируют оптимальный вариант осуществления изобретения. Данные чертежи, совместно с прилагаемым описанием, приведены для разъяснения принципов изобретения. На чертежах:

- на фиг.1 схематически представлена система, в которой терминал мобильной связи и сервер проверки приспособлены для работы в соответствии со способом по изобретению;
- на фиг.2 схематически представлена общая блок-схема, иллюстрирующая последовательность этапов от открытия/регистрации приложения в терминале мобильной связи до использования такого терминального приложения;
- на фиг.3 схематически представлена блок-схема, иллюстрирующая терминал мобильной связи, приспособленный для работы в соответствии со способом по изобретению;
- на фиг.4 схематически представлена блок-схема, иллюстрирующая порядок работы терминала мобильной связи по изобретению;
- на фиг.5 схематически представлена блок-схема, иллюстрирующая генерирование и использование терминального приложения;
- на фиг.6 схематически представлена блок-схема, иллюстрирующая процедуру проверки;
- на фиг.7 схематически представлена блок-схема, иллюстрирующая один из аспектов изобретения.

Осуществление изобретения

Ниже приводится подробное описание одного из примеров осуществления настоящего изобретения со ссылками на прилагаемые чертежи. Одинаковые элементы на различных чертежах насколько возможно обозначены одними и теми же цифровыми обозначениями.

На фиг.1 схематически представлена схема системы, в которой терминал мобильной связи работает в соответствии со способом по изобретению.

Система, представленная на фиг.1, содержит сеть 110 мобильной связи, например, сеть GSM, в которую входят несколько базовых станций, таких как базовая станция 111. Базовая станция 111 осуществляет обмен информацией с пользовательским терминалом 300 мобильной связи, например, представляющим собой мобильный телефон. Система дополнительно содержит клиентский компьютер 122, в котором предусмотрено приложение веб-клиента. Клиентский компьютер 122 и веб-сервер 124 в рабочем состоянии подключены к компьютерной сети 120, предпочтительно представляющей собой Интернет.

Для осуществления рабочего соединения между сетью 110 мобильной связи и компьютерной сетью 120 предусмотрен шлюз 116.

Сервер 112 поставщика услуг подключен в рабочем режиме к сети 110 мобильной связи. Сервер 112 поставщика услуг также соединен в рабочем режиме с сервером 130 проверки предпочтительно при помощи закрытого канала связи, например,

виртуальной частной сети 114. Специалистам в данной области очевидно, что виртуальная частная сеть 114 такого рода в оптимальном варианте осуществления может быть выполнена в форме части Интернета и, следовательно, части компьютерной сети 120. Для упрощения иллюстрации на фиг.1 виртуальная частная сеть представлена в виде отдельного соединения.

Сервер 130 проверки соединен в рабочем режиме с веб-сервером 124. Сервер 130 проверки и веб-сервер 124 могут быть расположены в одной и той же географической точке; в этом случае соединение 132 между ними может быть осуществлено с использованием локальной сети (LAN). В альтернативном варианте осуществления соединение 132 может быть осуществлено с использованием виртуальной частной сети. Специалистам в данной области очевидно, что виртуальная частная сеть 132 такого рода в оптимальном варианте осуществления может быть выполнена в форме части Интернета и, следовательно, части компьютерной сети 120. Для упрощения иллюстрации на фиг.1 виртуальная частная сеть 132 представлена в виде отдельного соединения.

Клиентский компьютер 122 снабжен веб-браузером. Таким образом, пользователь может при помощи клиента 122 осуществлять обмен информацией с другими компьютерами, подключенными к сети 120, например, с веб-сервером 124.

При помощи веб-браузера, установленного в клиентском компьютере 122, пользователь может проводить операции заказа и регистрации, выполняемые веб-сервером 124. Эти операции позволяют пользователю регистрироваться и заказывать загружаемое, специально приспособленное терминальное приложение для использования подписи и аутентификации при использовании услуг мобильной связи.

Обмен информацией между клиентским компьютером 122 и веб-сервером 124 в оптимальном варианте может осуществляться в зашифрованном виде, например, с использованием защищенного протокола защиты SSL (Secure Sockets Layer).

Таким образом, веб-сервер 124 приспособлен для генерирования специально приспособленного терминального приложения, содержащего исполняемый программный код, который может быть выполнен терминалом 300 мобильной связи. В качестве такого программного кода предпочтительно используют приложение J2ME (комплекс программ типа «мидлет»), содержащее необходимый код и другие данные. Это гарантирует универсальность решения относительно различных аппаратных платформ (переносимость).

При помощи сети 110 мобильной связи и поставщика 112 услуг можно установить канал связи между терминалом 300 мобильной связи и сервером 130 проверки. Для затруднения несанкционированного просмотра протоколов и несанкционированного доступа к сообщениям и/или подписям следует исключить доступ посторонних лиц к данному каналу. Это может быть осуществлено при помощи функций защиты/шифрования, встроенных в сеть 110 мобильной связи и в предпочтительное соединение 114 по виртуальной частной сети (VPN).

На фиг.2 представлена общая блок-схема последовательности этапов работы от регистрации заказа терминального приложения до реального использования терминального приложения.

Последовательность начинается с начального этапа 200.

Прежде всего выполняют операцию 202 заказа и регистрации. В ходе данной операции пользователь заказывает специально приспособленное терминальное приложения для использования в определенных целях. Оформление заказа обычно производят путем взаимодействия между клиентским компьютером 122 и веб-

сервером 124 по сети 120, обычно представляющей собой Интернет.

В ходе этапа 202 заказа и регистрации пользователь идентифицируется и регистрируется, после чего заказывает загружаемое терминальное приложение. Осуществляя обмен информацией с веб-сервером 124 при помощи клиентского компьютера 122, пользователь может выбрать требуемый тип приложения. В ходе этапа 202 заказа и регистрации требуемый тип приложения приписывается к идентификатору абонента услуг мобильной связи, предпочтительно к телефонному номеру, сообщенному пользователем. Веб-сервер 124 использует идентификатор абонента услуг мобильной связи в качестве адреса отправки сообщения, относящегося к загрузке, которое высылается на терминал 300 мобильной связи в связи с этапом 206 загрузки.

В ходе этапа 202 заказа и регистрации пользователь также предоставляет соответствующие регистрационные данные, например пароль или PIN-код, который также приписывают к конкретному терминальному приложению.

После этого выполняют следующий этап 204 производства или адаптации. В ходе этапа 204 производства или адаптации веб-сервер должен адаптировать заранее созданное терминальное приложение, содержащее исполняемый программный код, который может быть использован терминалом 300 мобильной связи. В качестве такого программного кода предпочтительно используют приложение J2ME (комплекс программ типа «мидлет»), содержащее необходимый код и другие данные.

Этап 204 адаптации начинается с использования заранее созданного программного кода терминального приложения, причем тип приложения выбран пользователем на этапе 202 заказа.

Этап 204 адаптации включает в себя операцию приписывания терминальному приложению идентификатора, уникального для данного терминального приложения.

Регистрационные данные, введенные пользователем на этапе 202 заказа, сохраняют в базе данных веб-сервера 124 со ссылкой на приписанный терминальному приложению уникальный идентификатор. Регистрационные данные предпочтительно сохраняют в зашифрованном виде.

Кроме того, этап 204 адаптации включает в себя операцию приписывания терминальному приложению базового ключа, также уникального для данного терминального приложения. Базовый ключ генерируют в ходе этапа адаптации, причем указанный базовый ключ создают на основе главного ключа, сохраняемого централизованно, и уникального идентификатора терминального приложения.

Кроме того, этап 204 адаптации включает в себя операцию маркировки программного кода с использованием уникального идентификатора и базового ключа. Данные, представляющие собой идентификатор, предпочтительно вводят в код терминального приложения прямым и открытым образом, а данные, представляющие собой базовый ключ, предпочтительно вводят в код терминального приложения скрытым образом. Термин «скрытый образ» означает здесь, что базовый ключ скрыт в коде таким образом, что его невозможно прочитать напрямую или извлечь из кода, например, путем декомпиляции.

Более подробное описание этапа 204 адаптации приведено ниже со ссылками на фиг.5.

Полученное в результате адаптированное терминальное приложение сохраняют на веб-сервере 124, предпочтительно в виде так называемого комплекса программ типа «мидлет».

На этапе 206 загрузки, представленном на фиг.2, генерируют служебное сообщение,

обычно в форме текстового сообщения SMS, которое отправляют на терминал 300 мобильной связи. Адресацию терминала 300 мобильной связи осуществляют при помощи вышеупомянутой идентификационной информации абонента услуг мобильной связи. Сообщение содержит ссылку на терминальное приложение, сохраненное на веб-сервере 124. При активации пользователем терминала такой ссылки производится загрузка терминального приложения с веб-сервера 124 на терминал 300 мобильной связи через сеть 120, шлюз 116 и сеть 110 мобильной связи.

После пересылки терминального приложения на терминал мобильной связи и, таким образом, получения терминалом мобильной связи возможности исполнения терминального приложения осуществляют этап 210 комплексного исполнения. Этот этап включает в себя две операции: операцию 212 подписания, осуществляемую на терминале мобильной связи, и операцию 214 проверки, осуществляемую на севере проверки.

Операция 212 подписания включает в себя исполнение пользователем загруженного специально приспособленного терминального приложения на соответствующем терминале мобильной связи. Операцию проверки осуществляют на сервере проверки с целью проверки подписи после осуществления операции подписания. Она, в свою очередь, может быть использована для проверки подлинности личности пользователя.

На фиг.3 схематично представлена схема, иллюстрирующая структурную архитектуру терминала мобильной связи, приспособленного для осуществления операций по изобретению.

Терминал 300 мобильной связи выполнен с использованием стандартной шинной архитектуры, в которой шина 302 соединена в рабочем режиме с процессором 320, модулем 330 памяти, модулем 310 идентификации абонента (SIM) в форме электронной смарт-карты, звуковым модулем 316, адаптером 312 дисплея, модулем радиосвязи или приемопередатчиком 350 и адаптером 304 входящих сигналов.

Адаптер 312 дисплея соединен с дисплеем 314. Приемопередатчик 350 соединен с антенной 352.

Адаптер 304 входящих сигналов приспособлен для приема информации, вводимой вручную при помощи системы ввода, например клавиатуры 306.

Модуль 330 памяти в частности приспособлен для сохранения в процессе работы терминала, помимо прочего, специально приспособленных терминальных приложений 340 (комплексов программ типа «мидлет»). Терминальное приложение содержит исполняемый программный код, который, в частности, содержит данные, представляющие собой базовый ключ, приписанный к терминальному приложению.

На фиг.4 схематически представлена блок-схема, иллюстрирующая операцию исполнения приложения терминалом мобильной связи в соответствии изобретением.

Данная операция выполняется процессором 320 терминала 300 мобильной связи с целью снабжения полученного сообщения электронной подписью. После этого подписанное сообщение может быть передано на сервер 130 проверки.

Осуществление способа начинают с начального этапа 400.

На этапе 402 получения происходит получение сообщения, предпочтительно от элемента поставщика услуг в терминале. В принципе, данное сообщение может представлять собой случайное сообщение или вызов, содержание которого не имеет смысла, например случайную последовательность байтов. На практике, особенно если способ по изобретению используют в приложении к системам заказов или платежей с использованием мобильной связи, сообщение может содержать данные, относящиеся к сделке, в частности, данные, представляющие собой договор между поставщиком 112

услуг и пользователем терминала 300 мобильной связи.

На этапе 404 из модуля памяти терминала извлекают базовый ключ. Более конкретно, базовый ключ извлекают из области памяти, содержащей часть кода терминального приложения, т.е. прикладную программу, загруженную в терминал. Данная часть кода, содержащая алгоритмы и данные, соответствующие базовому ключу, предпочтительно сохранена в памяти в скрытом виде.

Затем переходят к выполнению этапа 406, на котором из счетчика терминала мобильной связи, предпочтительно из постоянной памяти, извлекают значение счетчика. Значение счетчика увеличивают после его извлечения или в другой момент так, чтобы значения счетчика для каждого следующего выполненного этапа 412 формирования подписи (см. ниже) были различными.

Затем на этапе 408 осуществляют ввод регистрационных данных пользователя терминала мобильной связи. Пароль предпочтительно вводится пользователем с клавиатуры терминала или при помощи другой управляемой пользователем системы ручного ввода. В оптимальном варианте может использоваться цифровой пароль в форме, например, четырехзначного PIN-кода.

Дальнейшие операции предполагают использование базовой функции шифрования, которую используют для формирования ключа и подписи. В оптимальном варианте такая функция шифрования может быть основана на методе симметричной криптографии, например, на технологии 3DES.

На этапе 410 формируют динамический ключ, создаваемый на основе базового ключа, значения счетчика и регистрационных данных.

Этап 410 формирования ключа включает в себя использование заранее определенной функции шифрования при формировании динамического ключа. Базовый ключ, значение счетчика и регистрационные данные предпочтительно используют в качестве входных значений данной функции шифрования. В наиболее предпочтительном варианте динамический ключ формируют по следующей схеме:

$K_I^c = f(BK(i), c, PW)$,

где f(BK, c, P) - функция формирования уникального ключа шифрования,

BK(i) - базовый ключ,

PW - введенные регистрационные данные.

На следующем этапе 412 осуществляют формирование подписи, причем подпись для сообщения формируют с использованием динамического ключа. Этап 412 подписи включает в себя использование заранее определенной функции подписания сообщения, полученного на этапе 402 получения.

Функция подписания основана на базовой функции шифрования, описанной выше. Примеры подходящих функций подписания известны специалистам в данной области под названиями CBC-MAC и OMAC.

После этого предпочтительно выполняют этап 414, на котором неподписанное сообщение и полученную ранее подпись отсылают на сервер 130 проверки. Кроме того, отсылают значение счетчика и уникальный идентификатор терминального приложения.

Вышеописанная процедура гарантирует, что динамический ключ используют только временно и ограниченно, и только в операции подписания. Поэтому сохранение динамического ключа в каком бы то ни было месте в какой бы то ни было момент исключается. Кроме того, исключается сохранение регистрационных данных пользователя, например PIN-кода, в терминале мобильной связи. Эти характеристики изобретения способствуют повышению безопасности.

На фиг.5 представлена блок-схема, иллюстрирующая конкретный пример адаптации и использования терминального приложения.

Верхняя часть 504 фиг.5 иллюстрирует операцию адаптации, используемую для создания специально приспособленного терминального приложения. В приведенном выше описании со ссылками на фиг.2 данная операция 504 была обозначена номером 204. Операцию 204 производства обычно выполняют на веб-сервере 124 по завершении операции 202 заказа.

Нижняя часть фиг.5, обозначенная номером 500, иллюстрирует операцию подписания, выполняемую терминальным приложением. Операцию 500 подписания выполняют на терминале 300 мобильной связи; в приведенном выше описании со ссылками на фиг.2 данная операция была обозначена номером 212.

Ниже следует описание операции 504 адаптации:

Базовый ключ 532 получают на основе уникального идентификатора 510 и основного ключа 518. Базовый ключ 532 используют в качестве входных данных операции 500 подписания.

Ниже следует описание операции 500 подписания:

Динамический ключ 534 получают на основе регистрационных данных 520 пользователя, значения 524 счетчика и базового ключа 532. Динамический ключ 534 используют в качестве входных данных для операции 536 формирования подписи.

В ходе операции 536 формирования подписи сообщение 538 подписывают с использованием динамического ключа 534, в результате чего получают подпись 540.

На фиг.6 схематически представлена блок-схема, иллюстрирующая операцию 600 проверки.

Операция 600 проверки, по существу, включает в себя те же операции/этапы, что и операция 204 адаптации и операция 212 подписания. Аналогичные операции/этапы обозначены на фиг.5 и 6 одинаковыми номерами.

Операцию 600 проверки выполняют на сервере 130 проверки.

Входные данные операции проверки состоят из уникального идентификатора 510, значения 524 счетчика, неподписанного сообщения 538 и проверяемой подписи 540.

Цель операции 600 проверки заключается в формировании сигнала 604 подтверждения (который может принимать значения «истинно» и «ложно»), который указывает, является ли подпись 540 корректной подписью для сообщения 538, с учетом уникального идентификатора 510 терминального приложения и значения 524 счетчика.

Уникальный идентификатор 510, значение 524 счетчика, неподписанное сообщение 538 и подпись 540 получают от терминала мобильной связи после завершения терминалом мобильной связи операции подписания. Эти данные предпочтительно получают через сервер 112, расположенный у поставщика услуг.

Кроме того, в операции 600 проверки используют основной ключ 518, сохраненный на сервере 130 проверки.

Кроме того, операция 600 проверки имеет доступ к базе 606 данных сервера 130 проверки. База 606 данных содержит сохраненные в зашифрованном виде регистрационные данные пользователей (в частности, пароли или PIN-коды). Для расшифровки сохраненных в зашифрованном виде регистрационных данных предусмотрена операция 608 расшифровки, позволяющая получить расшифрованные регистрационные данные пользователя, соответствующие уникальному идентификатору 510.

Базовый ключ 525 получают в модуле 512 на основе уникального идентификатора 510 и основного ключа 518.

В модуле 522 получают динамический ключ на основе регистрационных данных 520 пользователя, значения 542 счетчика и базового ключа 525.

Регистрационные данные 520 пользователя формируют при помощи функции 608 расшифровки, как описано выше. Динамический ключ 534 используют в качестве входных данных для операции 536 формирования подписи.

В ходе выполнения операции 536 формирования подписи входящее сообщение 538 подписывают с использованием динамического ключа 534, в результате чего получают сформированную подпись 612.

На этапе 602 сравнения сформированную подпись 612 сравнивают с входящей подписью 540 для проверки идентичности данных подписей. Если подписи идентичны, сигналу 604 подтверждения присваивают значение true («истинно»). Если подписи не идентичны, сигналу 604 подтверждения присваивают значение false («ложно»).

На фиг.7 схематически представлена схема, иллюстрирующая другой аспект настоящего изобретения. Как показано на схеме, терминал 300 мобильной связи также может содержать дополнительный компонент 342, приспособленный для осуществления услуг, предоставляемых поставщиком 112 услуг, например услуг заказов или платежей с использованием мобильной связи.

Терминальное приложение может состоять из нескольких компонентов, но обычно состоит из двух компонентов. Они представляют собой компонент, предоставляемый поставщиком услуг, и компонент по настоящему изобретению, которые совместно образуют единое терминальное приложение, условно обозначенное на фиг.7 элементом 345.

Как показано на фиг.7, терминал 300 мобильной связи содержит приложение, которое может содержать два компонента, в число которых может входить загруженный компонент 340 подписания, взаимодействующий и обменивающийся информацией в рабочем режиме с компонентом 342 поставщика услуг. Оба компонента 340, 342 представляют собой исполняемые программные модули, которые (как показано на фиг.3) сохранены в памяти 330 терминала 300 мобильной связи. Как показано на фиг.7, неподписанное сообщение M передают от компонента 342 поставщика услуг компоненту 340 подписания, а подпись S, уникальный идентификатор uid и значение cnt счетчика возвращают компоненту 342 поставщика услуг. Подпись S, уникальный идентификатор uid, значение cnt счетчика и данные коммерческой операции, т.е. данные, связанные с предоставляемой услугой, и, в частности, данные, относящиеся к договору между пользователем и поставщиком услуг, передают по сети мобильной связи на сервер 112 поставщика услуг. После этого сервер поставщика услуг передает сообщение M, подпись S, уникальный идентификатор uid и значение cnt счетчика через канал 114 связи (например, представляющий собой виртуальную частную сеть VPN) на сервер проверки. Сервер проверки выдает сигнал 604 подтверждения, который возвращают на сервер 112 поставщика услуг, и который определяет принятие или непринятие сформированной подписи. Эта процедура может использоваться на сервере 112 поставщика услуг для проверки или аутентификации идентификации пользователя.

Для специалиста в данной области очевидно, что при интерпретации вышеприведенного подробного описания настоящего изобретения и при практическом осуществлении изобретения возможно внесение различных изменений и приспособлений.

Вышеизложенное подробное описание приведено с целью иллюстрации и описания оптимальных вариантов осуществления изобретения. Однако данное описание не

подразумевает ограничения изобретения подробно описанными вариантами его осуществления.

В описанном примере сеть 110 мобильной связи представляет собой сеть типа GSM. Однако следует понимать, что в изобретении равным образом могут быть использованы другие сети мобильной связи, например сети типа 3G или UMTS.

В описанном примере терминал 300 мобильной связи представляет собой мобильный телефон. Однако следует понимать, что в изобретении равным образом могут быть использованы другие типы терминалов мобильной связи, приспособленные для обмена информацией при помощи сети 110 мобильной связи, например устройства PDA или портативные персональные компьютеры.

Также следует понимать, что вышеупомянутое оптимальное использование приложения для терминала мобильной связи в форме приложения J2ME (комплекса программ типа «мидлет») наиболее целесообразно с точки зрения переносимости, т.е. возможности исполнения такого приложения на различных аппаратных платформах без внесения дополнительных изменений. Однако в рамках настоящего изобретения возможны и другие варианты осуществления такого приложения. В частности, терминальное приложение может быть написано на языке низкого уровня (объектном коде) или на других языках высокого уровня.

Для специалиста в данной области из вышеприведенного описания очевидно, что в настоящее изобретение могут быть внесены другие изменения и модификации. Охват изобретения очевидным образом следует из приведенных ниже пунктов формулы изобретения и их эквивалентов.

Формула изобретения

1. Способ создания электронной подписи, осуществляемый модулем процессора терминала мобильной связи, причем способ включает в себя следующие этапы:

извлекают базовый ключ из области памяти в терминале мобильной связи;

осуществляют ввод пользователем регистрационных данных;

формируют динамический ключ на основе базового ключа и регистрационных данных;

отличающийся тем, что способ дополнительно включает в себя следующие этапы:

получают электронное сообщение и

формируют электронную подпись с использованием сгенерированного динамического ключа,

причем этап извлечения базового ключа включает в себя получение базового ключа из области памяти, содержащей участок кода терминального приложения, загруженного на терминал мобильной связи, причем, по меньшей мере, базовый ключ сохранен в указанном участке кода в скрытом виде, при этом базовый ключ скрыт в коде таким образом, что его невозможно прочитать напрямую или извлечь из кода.

2. Способ по п.1, отличающийся тем, что этап формирования динамического ключа на основе базового ключа и регистрационных данных дополнительно основан на значении счетчика, извлеченном из счетчика терминала путем получения значения счетчика из открытой для чтения и записи памяти терминала.

3. Способ по одному из пп.1-2, отличающийся тем, что этап ввода регистрационных данных включает в себя получение от пользователя пароля.

4. Способ по одному из пп.1-2, отличающийся тем, что этап формирования динамического ключа включает в себя использование в качестве входных данных базового ключа, значения счетчика и регистрационных данных.

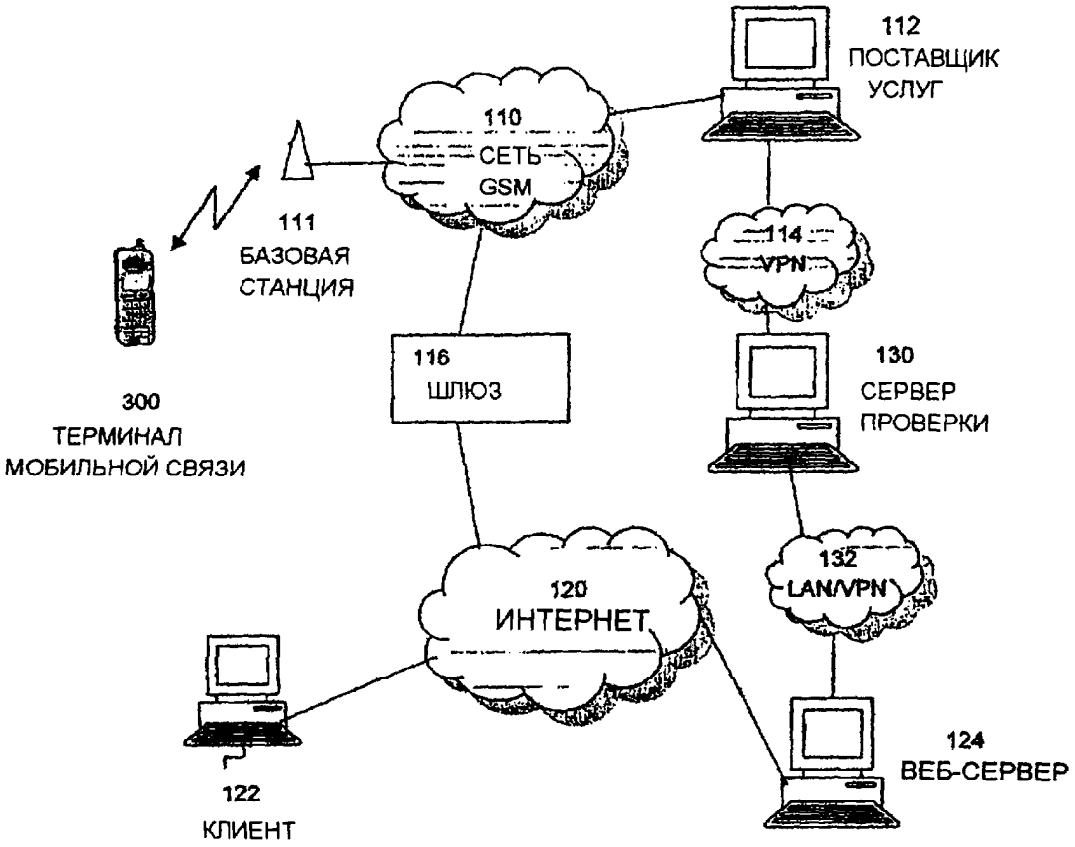
5. Способ по одному из пп.1-2, отличающийся тем, что дополнительно включает в себя следующий этап:

отсылают подписанное сообщение, содержащее электронное сообщение и сформированную подпись, на сервер проверки.

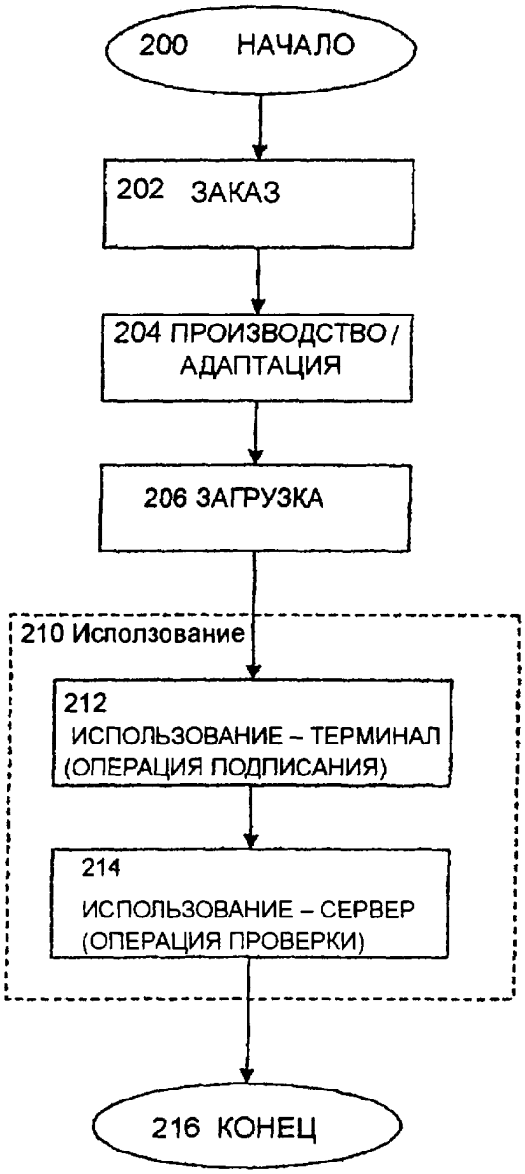
6. Способ по п.5, отличающийся тем, что значение счетчика и уникальный идентификатор также отсылают на сервер проверки.

7. Машиночитаемый носитель данных, содержащий программные инструкции, исполнение которых модулем процессора терминала мобильной связи вызывает осуществление модулем процессора способа по одному из пп.1-6.

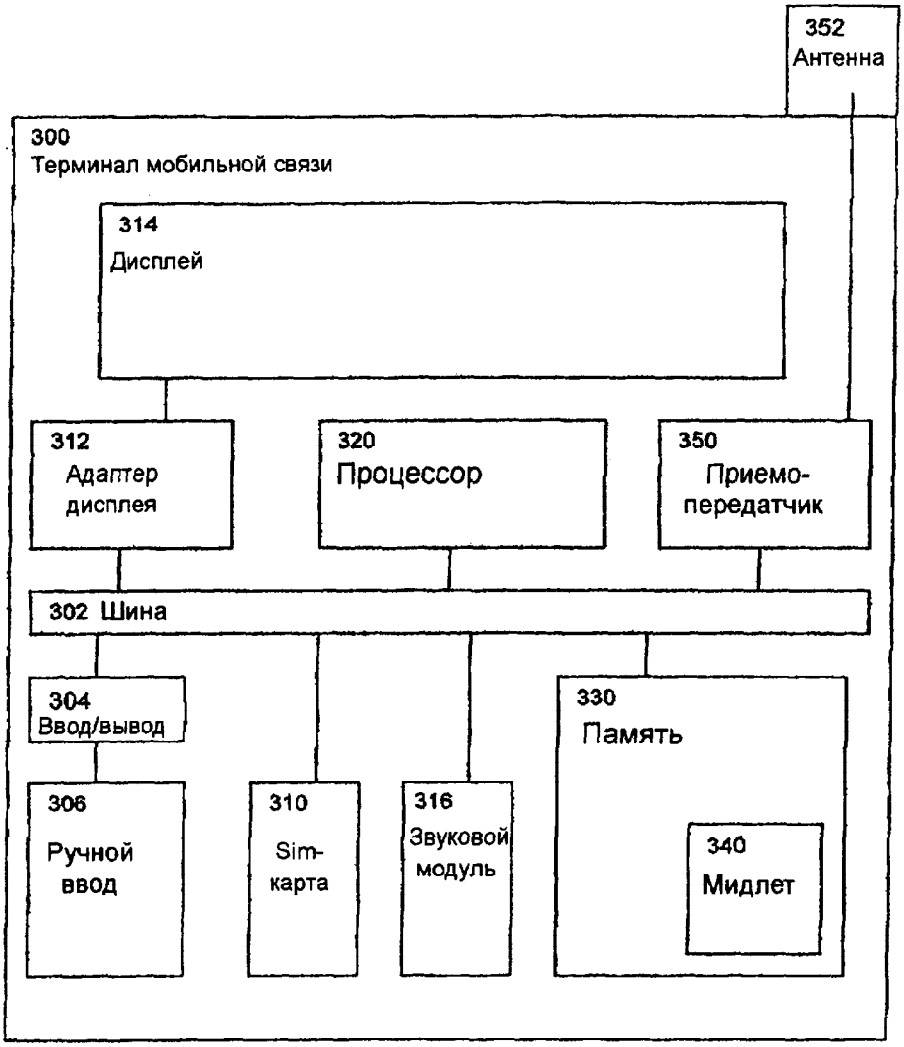
8. Терминал мобильной связи для создания электронной подписи, содержащий модуль процессора, выполненный с возможностью осуществления способа по одному из пп.1-6.


112
ПОСТАВЩИК
УСЛУГ
110
СЕТЬ
GSM
111
БАЗОВАЯ
СТАНЦИЯ
114
VPN
116
ШЛЮЗ
130
СЕРВЕР
ПРОВЕРКИ
300
ТЕРМИНАЛ
МОБИЛЬНОЙ СВЯЗИ
120
ИНТЕРНЕТ
132
LAN/VPN
122
КЛИЕНТ
124
ВЕБ-СЕРВЕР

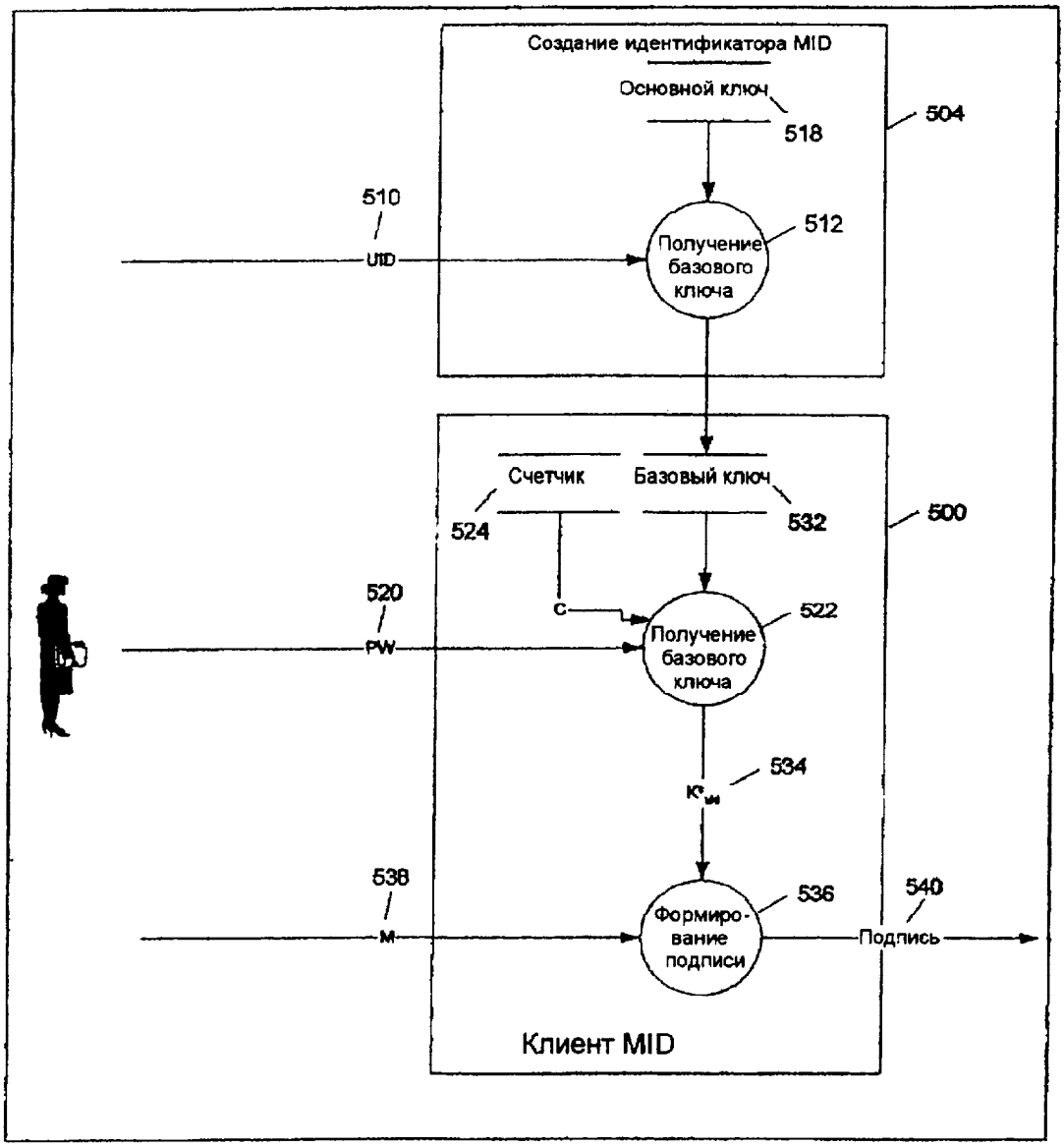
ФИГ. 1


200 НАЧАЛО
202 ЗАКАЗ
204 ПРОИЗВОДСТВО / АДАПТАЦИЯ
206 ЗАГРУЗКА
210 Исполозование
212 ИСПОЛЬЗОВАНИЕ – ТЕРМИНАЛ (ОПЕРАЦИЯ ПОДПИСАНИЯ)
214 ИСПОЛЬЗОВАНИЕ – СЕРВЕР (ОПЕРАЦИЯ ПРОВЕРКИ)
216 КОНЕЦ

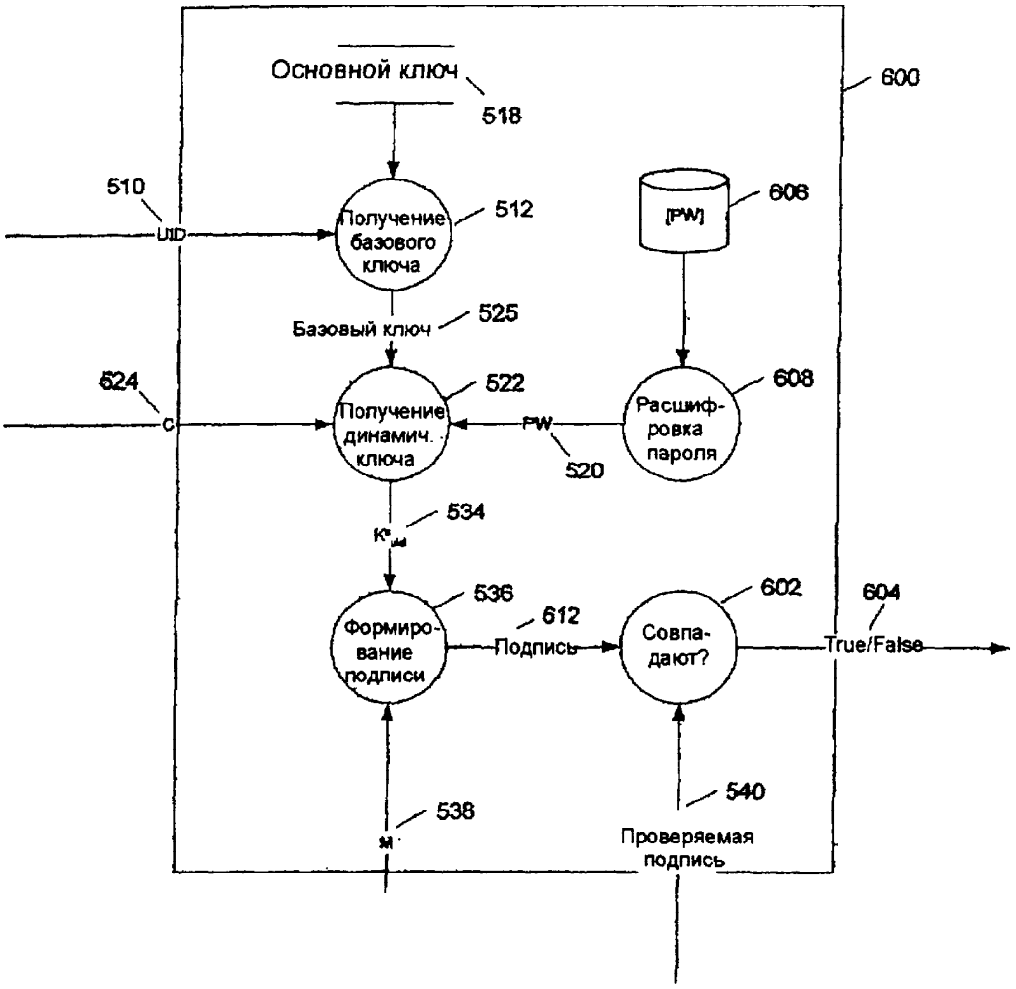
ФИГ. 2


352
Антенна
300
Терминал мобильной связи
314
Дисплей
312
Адаптер дисплея
320
Процессор
350
Приемо-передатчик
302 Шина
304
Ввод/вывод
306
Ручной ввод
310
Sim-карта
316
Звуковой модуль
330
Память
340
Мидлет

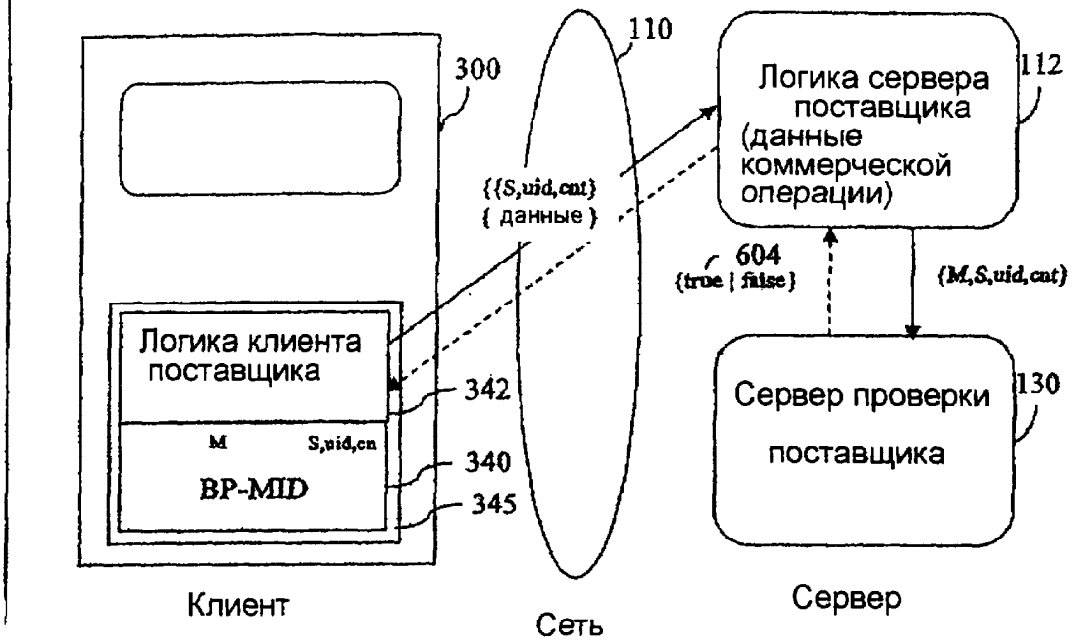
ФИГ. 3


Создание идентификатора MID
Основной ключ
518
504
510
UID
Получение базового ключа
512
Счетчик
Базовый ключ
524
532
500
C
520
PW
Получение базового ключа
522
534
538
M
Формирование подписи
536
540
Подпись
Клиент MID

ФИГ. 5


Основной ключ
518
600
510
UID
Получение базового ключа
512
[PW]
606
Базовый ключ
525
524
C
Получение динамич. ключа
522
PW
520
Расшифровка пароля
608
534
536
Формирование подписи
612
Подпись
602
Совпадают?
604
True/False
538
M
540
Проверяемая подпись

ФИГ. 6


300
110
Логика сервера поставщика (данные коммерческой операции)
112
{{S,uid,cnt} { данные }
604
{true | false}
{M,S,uid,cnt}
Логика клиента поставщика
342
M
S,uid,cn
BP-MID
340
345
Сервер проверки поставщика
130
Клиент
Сеть
Сервер

ФИГ. 7