РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 326 509** (13) **C2**

(51) МПК
H04Q 7/32 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2004115025/09, 02.12.2002**

(24) Дата начала отсчета срока действия патента:
02.12.2002

(30) Конвенционный приоритет:
04.12.2001 DE 10159398.8

(43) Дата публикации заявки: **10.11.2005**

(45) Опубликовано: **10.06.2008 Бюл. № 16**

(56) Список документов, цитированных в отчете о поиске: **EP 1107627 A, 13.06.2001. RU 99125207 A, 27.09.2001. US 5802175 A, 01.09.1998. EP 0730387 A, 04.09.1996. WO 00/39987 A1, 06.07.2000. EP 1107627 A1, 13.06.2001. WO 0059244 A1, 05.10.2000.**

(85) Дата перевода заявки PCT на национальную фазу:
05.07.2004

(86) Заявка PCT:
EP 02/13627 (02.12.2002)

(87) Публикация PCT:
WO 03/049471 (12.06.2003)

Адрес для переписки:
101990, Москва, Петроверигский пер., 4, "Агентство Ермакова, Столярова и Партнеры", пат.пов. Е.А.Ермаковой

(72) Автор(ы):
КИРШ Йохен (DE),
КЛААССЕН Ралф (DE),
ЭКАРДТ Стефан (DE)

(73) Патентообладатель(и):
ГИЗЕКЕ ЭНД ДЕВРИЕНТ ГмбХ (DE)

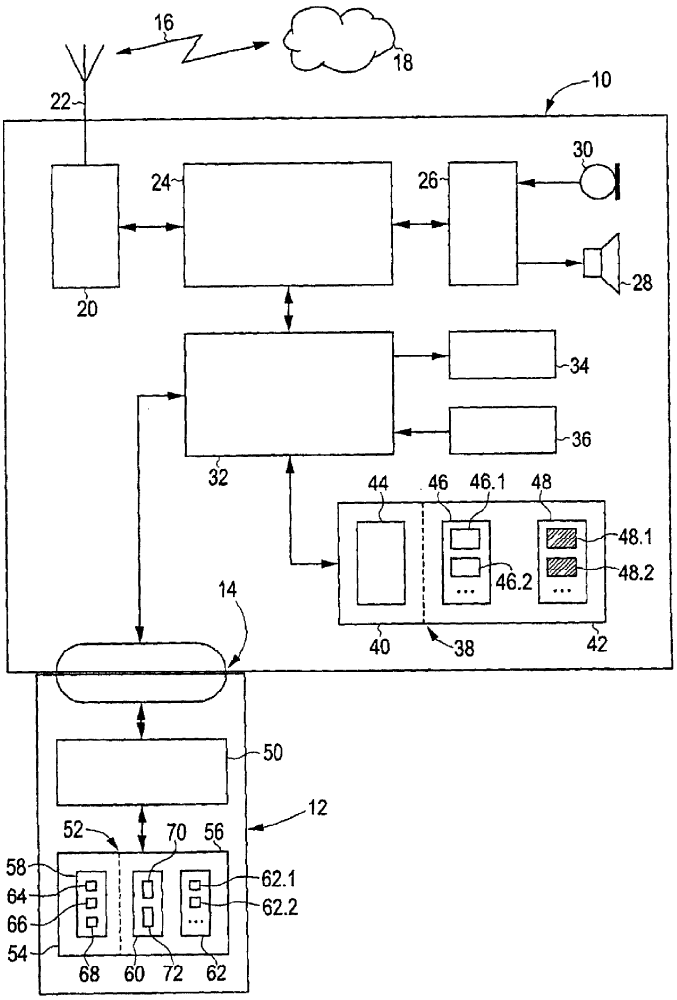
RU 2326509 C2

(54) СПОСОБ ХРАНЕНИЯ И ДОСТУПА К ДАННЫМ В МОБИЛЬНОМ УСТРОЙСТВЕ И МОДУЛЬ ПОЛЬЗОВАТЕЛЯ

(57) Реферат:

Изобретение относится к способам хранения и доступа к пользовательским данным и данным конфигурации в мобильном устройстве, соединенном с модулем пользователя. Технический результат состоит в повышении безопасности и усилении защиты от неавторизованного доступа к пользовательским данным и программам-приложениям в мобильном устройстве. Для этого пользовательские данные хранятся в мобильном устройстве, по крайней мере, в частично зашифрованном виде и расшифровываются при осуществлении операций доступа с помощью функции расшифровки модуля пользователя. Кроме того, данные конфигурации хранятся в модуле пользователя. Данные конфигурации указывают на то, разрешается ли мобильному устройству выполнить программу-приложение или в каком объеме разрешается выполнение такой программы. 6 н. и 27 з.п. ф-лы, 1 ил.

RU 2326509 C2



RU 2326509 C2

RU 2326509 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 326 509** (13) **C2**

(51) Int. Cl.
H04Q 7/32 (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2004115025/09, 02.12.2002**

(24) Effective date for property rights: **02.12.2002**

(30) Priority:
04.12.2001 DE 10159398.8

(43) Application published: **10.11.2005**

(45) Date of publication: **10.06.2008 Bull. 16**

(85) Commencement of national phase: **05.07.2004**

(86) PCT application:
EP 02/13627 (02.12.2002)

(87) PCT publication:
WO 03/049471 (12.06.2003)

Mail address:
**101990, Moskva, Petroverigskij per., 4,
"Agentstvo Ermakova, Stoljarova i Partnery",
pat.pov. E.A.Ermakovoj**

(72) Inventor(s):
**KIRSh Jokhen (DE),
KLAASSEN Ralf (DE),
EhKARDT Stefan (DE)**

(73) Proprietor(s):
GIZEKE EhND DEVRIENT GmbKh (DE)

(54) METHOD OF STORAGE OF AND ACCESS TO DATA IN MOBILE DEVICE, AND USER MODULE

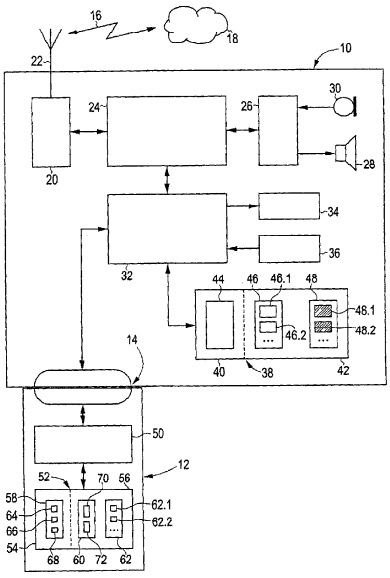
33 cl

(57) Abstract:

FIELD: physics, computing.

SUBSTANCE: invention relates to methods of storage of and access to user data and configuration data in a mobile device connected to a user module. The technical effect is the enhancement of security and protection against unauthorised access to user data and software applications in the mobile device. For that purpose, user data are stored in the mobile device in at least partially encrypted form and are decrypted during access operations using the user module decrypting function. Besides that, configuration data are stored in the user module. The configuration data determine if the mobile device is allowed to execute a certain software application and the scope of such application execution.

EFFECT: enhancement of security and protection against unauthorised access to data in mobile device.



RU 2326509 C2

RU 2326509 C2

Настоящее изобретение относится в целом к технической области хранения и доступа к данным в мобильных устройствах, а также в модулях пользователя в устройствах такого типа. Мобильные устройства, обеспечивающие пользователя функциями связи (например, передача речи и/или данных по телефонной сети) и программами-приложениями (например, расписание встреч или текстовый редактор), представляют собой предпочтительную область применения настоящего изобретения. Мобильные устройства такого типа, в частности, могут быть настроены как полнофункциональные мобильные телефоны или как персональные цифровые помощники (PDA).

Патентная заявка Германии DE 19724901 A1, опубликованная для целей ознакомления третьих лиц, описывает мобильный телефон стандарта GSM (GSM расшифровывается как глобальная система мобильной связи). Мобильный телефон состоит из блока управления, памяти устройства и интерфейса для модуля идентификации абонента (SIM-карты). Данные пользователя, такие как, например, списки адресов, данные по обороту денежных средств или прайс-листы, могут записываться в память устройства через линейную связь с компьютером. Также программы (которые подробно не описываются) можно загрузить в память устройства через линейное соединение и, впоследствии, выполнять их посредством мобильного телефона. Данные могут передаваться в форме, обеспечивающей целостность, или в зашифрованной форме.

При включении мобильного телефона стандарта GSM, обычно происходит проверка авторизации, при которой пользователь должен ввести личный секретный номер (PIN, расшифровывается как личный идентификационный номер). Полный пользовательский интерфейс с опцией доступа к пользовательским данным, хранящимся в мобильном телефоне, запускается только в том случае, если секретный номер введен правильно. Большая часть пользовательских данных, таким образом, в определенной степени защищена. Тем не менее, существует проблема того, что достаточно компетентные правонарушители могут обойти такую защиту. Элементы памяти мобильных телефонов можно, например, считать напрямую на уровне аппаратного программного обеспечения с использованием соответствующих устройств.

Очень выгодно хранить пользовательские данные в мобильном устройстве при условии, если мобильное устройство также настроено на выполнение программ-приложений для обработки указанных пользовательских данных. Полнофункциональные мобильные телефоны, работающие в стандарте GSM, и персональные цифровые помощники (PDA) в настоящее время обладают такими функциями. Благодаря высоким скоростям передачи мобильных устройств поколения 2,5 и 3, таких, например, как устройства, поддерживающие сети GPRS (услуга общей пакетной радиосвязи), EDGE, UMTS (универсальная система мобильной связи) и WCDMA (диапазонный коллективный или многостанционный доступ с кодовым разделением каналов), программы-приложения можно загружать и/или обновлять через провайдера услуг в мобильные устройства через радиоинтерфейс.

Использование таких мобильных устройств влечет множество проблем и требует усовершенствования по множеству аспектов. В первую очередь, необходимо предотвратить неавторизованный доступ к программам-приложениям. Таким образом, должно быть гарантировано, что только авторизованный пользователь сможет вызвать программу-приложение или отдельные защищенные функции в программе-приложении. Во-вторых, было бы желательно предлагать пользователю возможность выбора функций, которые в максимальной степени соответствовали бы его требованиям. В-третьих, предоставленные функции должны в наименьшей степени зависеть от устройства.

Целью настоящего изобретения является полное или частичное решение описанных проблем. Настоящее изобретение, в частности, призвано повысить безопасность и защищенность от неавторизованного доступа к данным пользователя и программам-приложениям в мобильном устройстве. В предпочтительных вариантах изобретение также должно обеспечивать высокую степень удобства для пользователя и предоставлять возможность рентабельного внедрения.

В соответствии с изобретением, данная цель полностью или частично достигается посредством способа с признаками, отраженными в пунктах формулы изобретения 1 и 16 соответственно; мобильного устройства с признаками, отраженными в пунктах формулы изобретения 14 и 31 соответственно, и пользовательского модуля с признаками, отраженными в пунктах формулы изобретения 15 и 33 соответственно. Зависимые формулы изобретения относятся к предпочтительным вариантам воплощения изобретения.

Настоящее изобретение берет свое начало от базовой идеи удовлетворения ранее упомянутых требований к безопасности хранения пользовательских данных и данных настройки, соответственно, приемлемым способом.

Первый аспект изобретения относится к хранению пользовательских данных. Такие данные согласно изобретению хранятся в зашифрованном виде в памяти мобильного устройства. Соответствующие функции, обеспечивающиеся пользовательским модулем, используются, как минимум, чтобы расшифровать (а в предпочтительных вариантах также и зашифровать) пользовательские данные.

Поскольку все пользовательские данные в памяти мобильного устройства находятся только в зашифрованном виде, такие данные защищены от постороннего вмешательства даже в случае, если неавторизованный пользователь обойдет обычный пользовательский интерфейс мобильного устройства, чтобы получить доступ к содержимому в памяти устройства. Память устройства, как правило, весьма велика и может использоваться для хранения пользовательских данных без опасений за их безопасность, в силу этого относительно большие объемы данных и сложные структуры данных могут переноситься в мобильном устройстве.

Пользовательские данные, предназначенные для хранения в соответствии с настоящим изобретением, могут быть любыми по желанию пользователя. Предпочтительно это данные, подлежащие обработке программой-приложением, которая имеется в мобильном устройстве, такой как, например, график встреч и адресов для обработки расписанием встреч, имеющим функцию адресной книги, бизнес-таблицы, подлежащие обработке, например, программами табличных вычислений, голосовые данные, созданные, например, программами, записывающими речь, или тексты общего плана для обработки текстовыми редакторами. Может также возникнуть потребность в хранении пользовательских данных, для которых не имеется соответствующей программы-приложения на мобильном устройстве. В таком случае мобильное устройство выполняет роль безопасного носителя данных для переноса пользовательских данных, например, с рабочего на домашний компьютер.

В предпочтительных конфигурациях полностью или частично выполняются функции шифрования и расшифровки процессором пользовательского модуля, при этом процессор получает доступ к ключам, содержащимся в памяти модуля. В такой конфигурации не требуется выводить ключевые данные за пределы пользовательского модуля, что обеспечивает достижение особенно высокой степени безопасности. Такая проблема возникает, в частности, если ключевая информация также генерируется в пользовательском модуле и записывается в память модуля. Тем не менее, настоящее изобретение предусматривает также варианты, в которых, по меньшей мере, полностью или частично выполняется операция шифровки, а также (дополнительно) и расшифровке пользовательских данных процессором мобильного устройства, на которое функции шифровки и/или расшифровки переносятся из пользовательского модуля.

Предпочтительно используется способ асимметричного шифрования, например способ Райвеста-Шамира-Эдельмана (RSA). В этом случае ключевые данные содержат открытый и секретный ключи. Тем не менее, возможны конфигурации, в которых используются и способы симметричного шифрования. В целях описания концепции в таких конфигурациях ссылка также делается на "функции шифрования и расшифровки", даже несмотря на то, что в обоих случаях выполняются аналогичные этапы вычислений.

Согласно изобретению пользовательский модуль требуется, как минимум, для

выполнения этапов расшифровки. Это само по себе обеспечивает определенную степень защиты, поскольку пользовательский модуль и мобильное устройство могут находиться по отдельности друг от друга. В предпочтительных вариантах изобретения, тем не менее, функция расшифровки не включается, по крайней мере, если только не будет введено слово-пароль (или фраза-пароль) и/или проведен биометрический тест, как, например, проверка отпечатка пальца или анализ речи. Благодаря этой мере гарантируется защищенность данных даже в случае потери мобильного устройства или пользовательского модуля.

Второй аспект изобретения касается использования данных конфигурации при выполнении программы-приложения в мобильном устройстве. Этот аспект основывается на базовой идее указания, посредством данных конфигурации, на наличие программы-приложения в полном объеме или отдельных функций программы-приложения. Данные конфигурации хранятся в пользовательском модуле, тогда как программа-приложение расположена в мобильном устройстве. Программа-приложение выполняется, только если она указана в данных конфигурации, или в том размере, в каком указана в этих данных.

Принципиально новый способ, отраженный в настоящем изобретении, предлагает защиту от неавторизованного выполнения программы-приложения или отдельных функций программы, поскольку в дополнение к мобильному устройству обязательно требуется пользовательский модуль с соответствующими данными настройки (конфигурации), позволяющими выполнять программы. Настоящее изобретение также создает техническую основу для создания конфигурации программы, настроенной в точном соответствии с требованиями пользователя. Это важно, в особенности, если необходима оплата за пользование программой, которая зависит от предоставленных функциональных возможностей, как, например, в случае со схемами ASP (ASP расшифровывается как услуга по прокату приложений). Поскольку в соответствии с настоящим изобретением данные конфигурации хранятся в пользовательском модуле, пользователь может настраивать необходимую ему конфигурацию в любом совместимом мобильном устройстве, просто подключившись вилкой к пользовательскому модулю.

Термин "программа-приложение", использующийся в данном описании, относится, в частности, к программам, которые выполняют функции обработки данных по отношению к пользовательским данным, упомянутым ранее. Если мобильное устройство является устройством, обладающим функциями связи, предпочтительно, чтобы программы-приложения не зависели от этих функций связи, либо могли, по меньшей мере, также использоваться и для других целей. Примерами типичных программ-приложений являются расписания встреч, адресные книги, текстовые редакторы, программы табличных вычислений, базы данных, программы для записи речи и другие. Термин "программы-приложения", использующийся в данном описании, также подразумевает программы, которые предусматривают только пользовательские интерфейсы вышеперечисленных или аналогичных приложений (в то время как обработка реальных данных выполняется на сервере провайдера услуг по прокату приложений - провайдера ASP-услуг). В некоторых конфигурациях также имеются браузеры и приложения для просмотра, позволяющие отображать документы в отформатированном виде как и программы-приложения. Однако программы-приложения могут также функционировать в качестве программ для воспроизведения мультимедийных файлов, например, в формате MP3.

С целью дальнейшего повышения защиты от неавторизованого выполнения программ-приложений отображение данных настройки (конфигурации) предпочтительно защищаются паролем и/или биометрическим тестом, таким как, например, анализ голоса или отпечатка пальца. В этом случае пользовательский модуль лишь отображает данные конфигурации и, таким образом, обеспечивает выполнение соответствующей программы-приложения или соответствующей функции программы, если пользователь предоставляет достаточное подтверждение своей личности посредством пароля и/или своих биометрических данных.

Функциональные возможности, обеспечиваемые настоящим изобретением, могут также использоваться в мобильных устройствах, которые содержат одну или несколько постоянно

хранящихся программ-приложений. Данные конфигурации, однако, предпочтительно также использовать для управления загрузкой программ-приложений или, по меньшей мере, их частей, - в мобильное устройство. В мобильные устройства с мощными функциями беспроводной передачи данных, программы-приложения или необходимые программные модули, в частности, могут загружаться от внешнего провайдера услуг через радиоинтерфейс. Эта возможность является особенно важной при совместном использовании со схемами ASP (услугами по прокату приложений). Для пользователя гораздо удобнее, когда он может автоматически загружать необходимые программы-приложения, соответствующие его конфигурации, просто путем использования пользовательского модуля или любого совместимого мобильного устройства. Вторичная загрузка программ-приложений поддерживается посредством использования языков программирования, которые работают независимо от платформы компьютера, как например, языка Java®.

Представляется особо выгодным сочетание двух вышеуказанных аспекта изобретения, поскольку в таком виде они обеспечивают защиту от неавторизованного доступа к данным пользователя и защиту от неавторизованного выполнения программ-приложений.

В предпочтительных конфигурациях, отражающих два упомянутых выше аспекта, мобильное устройство является устройством связи, в частности мобильным телефоном или персональным цифровым помощником (PDA) с функцией телефона. Пользовательский модуль предпочтительно является модулем идентификации абонента (SIM-картой), в соответствии с требованиями для входа в сеть телефонной связи. Пользовательский модуль, в частности, может обеспечиваться защитой от манипуляций, будучи так называемым "устройством с высоким уровнем надежности" или "устройством, защищенным от несанкционированного вмешательства", таким образом, что функции шифрования и расшифровки, либо зашифрованные данные или конфиденциальные данные конфигурации защищены от постороннего вторжения. Модуль идентификации абонента (SIM-карта) может использоваться, даже если мобильное устройство не имеет никаких функций телефонной связи или модуль не зарегистрирован у провайдера телефонной связи, поскольку модули такого типа производятся в больших количествах и, таким образом, реализуются по сравнительно низкой цене.

Мобильное устройство и пользовательский модуль предпочтительно дополняют признаками, которые соответствуют вышеописанным характеристикам и/или признакам, перечисленным в зависимых пунктах формулы изобретения, относящихся к способу.

Иные характеристики, преимущества и цели изобретения станут очевидными из последующего подробного описания варианта воплощения изобретения и множества альтернативных вариантов. Ссылки будут делаться на чертеж, представляющей блок-схему основных функциональных составляющих системы в соответствии с вариантом воплощения изобретения, описанным далее.

На чертеже изображено мобильное устройство 10 и модуль пользователя 12, соединенные друг с другом через интерфейс 14. В настоящем варианте изобретения мобильное устройство 10 имеет конфигурацию полнофункционального мобильного телефона, обеспеченного функцией связи в стандарте GSM, обеспечивающем поддержку телефонной связи, и стандарте GPRS для поддержки передачи данных. Модуль пользователя 12 соответственно имеет конфигурацию SIM-карты, вставленной в мобильный телефон или закрепленной в нем. Мобильное устройство 10 имеет доступ к соответствующей сети телефонной связи 18 через радиоинтерфейс 16. В альтернативных вариантах мобильное устройство 10 имеет конфигурацию, соответствующую усовершенствованному стандарту телефонной связи, такому как UMTS, и/или конфигурацию персонального цифрового помощника (PDA), который также может располагать возможностью воспроизводства мультимедийных данных.

Общеизвестно, что мобильное устройство 10 содержит высокочастотный элемент 20, который посылает и принимает радиоволны через антенну 22. Процессор цифровых сигналов (DSP) 24 используется для обработки передаваемых или полученных сигналов.

Процессор цифровых сигналов 24 также обрабатывает низкочастотные сигналы, направленные на громкоговоритель 28 через низкочастотный элемент 26 или отправленные с микрофона 30 через низкочастотный элемент 26 в процессор цифровых сигналов 24. Процессор 32 координирует все операции, происходящие в мобильном устройстве 10. Процессор 32 связан с интерфейсом 14, процессором цифровых сигналов 24, дисплеем 34, в данном случае имеющим конфигурацию жидкокристаллического дисплея, поддерживающего графическое изображение, клавиатурой 36 и памятью 38. Память 38 может быть постоянно установлена в мобильном устройстве или извлекаться из него, имея, например, форму платы памяти.

Память 38 формируется с использованием различных технологий, связанных с памятью, посредством множества полупроводниковых плат. В концептуальном изображении на чертеже память 38 состоит из области постоянного запоминающего устройства, ПЗУ 40 (реализованного, например, в виде запрограммированного фотошаблонами ПЗУ) и области памяти с возможностью перезаписи 42, реализованной, например, в виде ОЗУ (RAM), или электронно-перепрограммируемого ПЗУ (EEPROM), или флэш-памяти (FLASH). Область ПЗУ 40 памяти 38 содержит, в частности, действующие программы 44, выполняемые процессором 32, являющимся базовой операционной системой мобильного устройства 10; а также программы для реализации телекоммуникационных функций. Программы-приложения 46 и пользовательские данные 48 загружаются в память с возможностью перезаписи 42.

На чертеже показаны, в качестве примера программы-приложения 46, расписание встреч 46.1 (с функцией адресной книги) и текстовый редактор 46.2. Список встреч и адресов 48.1 для расписания встреч 46.1 и письмо 48.2 для текстового редактора 46.2 на чертеже показаны в качестве пользовательских данных 48. Программы-приложения 46 выполняются процессором 32 и имеют доступ к пользовательским данным 48. Пользовательские данные 48 хранятся в зашифрованном виде в памяти 38, как показано штриховкой на чертеже.

Модуль пользователя 12 имеет конфигурацию SIM-карты (модуля идентификации абонента) для сети телефонной связи 18, а интерфейс 14 также соответствует по своим механическим и электрическим свойствам стандартам, поддерживающимся этой сетью телефонной связи 18. Модуль пользователя 12 содержит процессор 50, имеющий конфигурацию микроконтроллера, интегрированного с памятью модуля 52 на отдельной плате (чипе). Память модуля 52 подразделена с использованием различных технологий памяти на ПЗУ 54 и память с возможностью перезаписи 56.

Память модуля 52 содержит управляющие программы и данные, которые, в первую очередь, обеспечивают основные функции операционной системы для модуля пользователя 12, а во вторую очередь, - вход в сеть и работу мобильного устройства 10 в сети телефонной связи 18. С целью упрощения описания эти управляющие программы и данные не показаны отдельно на чертеже. Шифровальные функции 58 в ПЗУ 54 в памяти модуля 52, ключевые данные 60 и данные конфигурации 62 в памяти с возможностью перезаписи 56 наиболее важны по отношению к вытекающим из настоящего изобретения аспектам варианта, описанного здесь, и поэтому они показаны на чертеже.

Шифровальные функции 58 состоят из функции шифрования 64, функции расшифровки 66 и функции генерации ключевых данных 68. Ключевые данные 60 подразделяются на открытый ключ 70 и секретный ключ 72. Данные конфигурации 62 состоят из соответствующей записи данных конфигурации для каждой программы-приложения 46, имеющейся в мобильном устройстве 10, то есть в варианте изобретения, описанном здесь, из записи о конфигурации 62.1 для расписания встреч 46. и записи о конфигурации 62.2 для текстового редактора 46.2.

В работе система, показанная на чертеже, обеспечивает обычные телекомуникационные функции, соответствующие необходимым стандартам, в настоящем случае стандарту GSM и GPRS. Вдобавок, пользователь может запускать программы-приложения 46 и обрабатывать пользовательские данные 48 и другие данные, содержащиеся в мобильном

устройстве.

Чтобы обеспечить работу программ-приложений 46, мобильное устройство 10 обращается к данным конфигурации 62 в модуле пользователя 12, когда мобильное устройство 10 включено или, по крайней мере, когда пользователь желает запустить программу-приложение 46. Такое обращение происходит через процессор 50 модуля пользователя 12, который, в свою очередь, требует ввода пароля перед тем, как обеспечить доступ к данным. Запрос пароля отображается на дисплее 34 мобильного устройства 10, и пользователь вводит соответствующий пароль с клавиатуры 36. Процессор 50 проверяет введенный пароль на правильность.

Если пользователь ввел правильный пароль, модуль пользователя 12 передает запрошенные данные конфигурации 62 (либо все данные конфигурации 62, либо только записи о конфигурации 62.1, 62.2 для соответствующих программ-приложений 46.1, 46.2) на мобильное устройство 10. Процессор затем проверяет, можно ли, в соответствии с переданными данными конфигурации 62, 62.1, 62.2, выполнить программы-приложения 46 или отдельно запрошенные программы-приложения 46.1, 46.2. Если они выполнимы, то выполнение программы разрешается.

Если необходимая программа-приложение 46.1, 46.2 уже находится в памяти 38, программа может быть запущена немедленно. В противном случае, необходимая программа или пользовательские данные, за которые может взиматься плата, загружаются в память 38 через радиоинтерфейс 16 и сеть телефонной связи 18 с сервера провайдера ASP-услуг (услуг по предоставлению приложений в аренду). Этот процесс загрузки также должен быть авторизован посредством модуля пользователя 12, который выполняет роль так называемого "сторожа". Даже если необходимая программа-приложение 46.1, 46.2 уже содержится в памяти 38, запрос, тем не менее, может исходить от провайдера услуг ASP, через радиоинтерфейс 16, сначала, на передачу биллинговых данных, а затем, - на импорт обновлений каких-либо программ, которые могут быть доступны для загрузки в мобильное устройство 10.

В описываемом варианте воплощения изобретения данные конфигурации 62 имеют отношение не только к основным авторизациям пользователя, но также и к предпочтительным настройкам программ-приложений 46, как, например, предварительно заданные пути файлов, настройки языка, настройки меню и прочие настройки пользователя. Такие настройки возможны при запуске программы-приложения 46 с тем, чтобы пользователь всегда работал с нужной ему конфигурацией программы. Эта возможность также реализуется, даже если пользователь подсоединит свой модуль пользователя 12 к новому или другому мобильному устройству 10.

Если программные интерфейсы приложений (API) станут достаточно стандартизированными, как ожидается в скором времени, например, с использованием языка программирования Java®, провайдеры ASP-услуг смогут предлагать услуги по индивидуальной настройке для каждого пользователя программ-приложений с обеспечением их независимости от используемого мобильного устройства 10. Высокий уровень безопасности также будет достигнут, поскольку все программы-приложения 46 могут быть вызваны только при условии, что имеется модуль пользователя 12 и пароль введен. Чтобы предотвратить неправомерное использование мобильного устройства 10, в случае его хищения во включенном состоянии (после того, как пользователь ввел пароль), устройство может быть снабжено опцией, согласно которой в случае, если пользователь не применял устройство в течение определенного промежутка времени, необходимо заново вводить пароль, наподобие того, как, например, это уже распространено в случае с скрин-сейверами (программами, отвечающими за экономичное использование экранов) для офисных компьютеров, которые не используются какое-то время.

В описываемом варианте воплощения изобретения программа-приложение 46 принимается за наименьшую единицу по отношению к механизму авторизации и, по выбору, по отношению к процессу загрузки через радиоинтерфейс 16. В зависимости от

применяемой технологии программирования, может использоваться более точный уровень детализации. Данные конфигурации 62 могут, таким образом, соотноситься с авторизацией пользователя для выполнения отдельных функций программ или отдельных программных модулей, к примеру, эти функции программ или программные модули могут, если нужно, загружаться по-отдельности через радиоинтерфейс 16. Такой подход позволяет, во-первых, избежать длительной загрузки, а во-вторых, обеспечить более точную пользовательскую настройку. Кроме того, при обновлении программ-приложений 46 через радиоинтерфейс 16 предпочтительно, чтобы передавались только программные модули, которые действительно изменились по сравнению с уже имеющейся в мобильном устройстве 10 версией.

Пользовательские данные 48, обработанные программами-приложениями 46, хранятся в памяти 38 полностью или, по меньшей мере, частично в зашифрованном виде. Пользователь может, например, иметь системы файлов для хранения пользовательских данных 48, в которых отдельные папки или отдельные диски выборочно настроены для хранения зашифрованных или незашифрованных данных. Аналогичная функциональная возможность для стационарных офисных компьютеров, в которых не применяется пользовательский модуль, уже известна на примере продукта PGPdisk®, производитель - "Нетуорк Ассоушиэйтс Инк." (Network Associates, Inc.).

Если программа-приложение 46 использовалась для хранения пользовательских данных 48 в области системы файлов, поддерживающих шифрование, то такие данные передаются из процессора 32 через интерфейс 14 в модуль пользователя 12. Процессор 50 модуля пользователя 12 выполняет функцию шифрования 64, в которой используется открытый ключ 70, содержащийся в системе ключевых данных 60. Зашифрованные пользовательские данные 48 записываются в память 38 посредством интерфейса 14 и процессор 32.

Доступ к пользовательским данным 48, которые хранились в зашифрованной форме, можно получить соответствующим способом. Здесь также процессор 50 модуля пользователя 12 выполняет расшифровку с использованием функции расшифровки 66 и секретного ключа 72. Однако перед тем, как выполнить эту операцию, процессор 50 запрашивает у пользователя фразу-пароль. Только при условии ввода правильного пароля с клавиатуры 36 (или, в ином случае, правильной идентификации пользователя посредством биометрического теста) выполняется процесс расшифровки.

В описываемом варианте изобретения шифрование и расшифровка выполняются асимметричным методом RSA. В альтернативных вариантах, напротив, используются другие методы асимметричного и симметричного шифрования и расшифровки, либо их смешанные вариации, как, например, симметричное шифрование с использованием асимметрично зашифрованного ключа. В симметричных методах нет необходимости различать открытый ключ 70 и секретный ключ 72.

Суммируя сказанное, можно сказать, что предложенная технология гарантирует, что зашифрованные пользовательские данные 48 могут быть считаны или использованы только в случае, если модуль пользователя 12 авторизованного пользователя соединен с интерфейсом 14, и пользователь правильно идентифицировался, например, с помощью пароля-фразы.

В настоящем варианте весь процесс шифрования и расшифровки выполняется процессором 50 модуля пользователя 12, причем ключевые данные 60 никогда не выходят за пределы модуля пользователя 12. Тем не менее, имеются альтернативные конфигурации, в которых функция шифрования 64 и открытый, несекретный ключ 70 сообщаются мобильному устройству 10 таким образом, что процесс шифрования выполняется, как правило, более мощным процессором 32 мобильного устройства. В некоторых альтернативных конфигурациях процессор 32 может также использоваться для процесса расшифровки при условии, что при этом не нарушается безопасность секретного ключа 72.

В настоящем варианте изобретения функция генерации 68 ключевых данных, которая

также выполняется процессором 50 модуля пользователя 12, используется в целях создания ключевых данных 60. Общеизвестным способом эта программа вычисляет пару, состоящую из открытого ключа 70 и секретного ключа 72. Эта мера гарантирует очень высокую степень безопасности данных, поскольку открытый ключ 72 не выходит за пределы модуля пользователя 12 даже, когда ключи генерируются.

Описанный здесь вариант воплощения изобретения не ограничивается - ни одной зашифрованной областью для пользовательских данных 48, ни одним способом шифровки. При условии, что соответствующее доказательство идентификации было предоставлено посредством фразы-пароля, зашифрованная область может быть, например, в любое время дезактивирована, и таким образом обеспечивается свободный доступ. Эта область может также вновь быть зашифрована посредством того же самого или другого модуля пользователя 12. Можно также устанавливать и управлять множеством зашифрованных областей, по выбору, - с различными парами ключей и/или различными размерами. В настоящей конфигурации, в частности, поддерживающей услуги ASP-провайдера, зашифрованные пользовательские данные 48 могут, помимо хранения в мобильном устройстве 10, также передаваться через радиоинтерфейс 16 на сервер ASP-провайдера и храниться в нем. Пользовательские данные 48, хранящиеся у обеих сторон, могут синхронизироваться каждый раз, когда программа-приложение 46 обеспечивает письменный доступ, или если пользовательский сеанс закончился, или когда это прямо запрашивается пользователем. Пользователь, таким образом, с одной стороны, получает быстрый доступ к локально хранящимся пользовательским данным 48, а с другой стороны, он не зависит от используемого мобильного устройства 10, поскольку он может также извлекать пользовательские данные 48, которые хранятся у провайдера ASP-услуг, с помощью любого другого мобильного устройства.

В некоторых конфигурациях может также поддерживаться возможность хранения элемента ключа у оператора сети или провайдера ASP-услуг. После того как мобильное устройство 10 успешно вошло в сеть телефонной связи 18, этот элемент ключа передается через радиоинтерфейс 16, так что управление определенными пользовательскими данными 48, хранящимися в мобильном устройстве, разделяется между оператором сети или ASP-провайдером и пользователем.

Формула изобретения

1. Способ хранения и доступа к пользовательским данным (48) в мобильном устройстве (10), в частности в мобильном телефоне или персональном цифровом помощнике, где мобильное устройство (10) содержит память (38) и подсоединено к модулю пользователя (12) через интерфейс (14), отличающийся тем, что:

пользовательские данные (48) хранятся в памяти (38) мобильного устройства (10), по крайней мере, в частично зашифрованном виде, по крайней мере, расшифровка пользовательских данных (48) в операциях доступа выполняется с использованием функции расшифровки (66), которая обеспечивается модулем пользователя (12) и,

по крайней мере, частично выполняется процессором (50) модуля пользователя.

2. Способ по п.1, отличающийся тем, что шифрование пользовательских данных (48) при осуществлении операций хранения выполняется с помощью функции шифрования (64), обеспечивающейся модулем пользователя (12).

3. Способ по п.1 или 2, отличающийся тем, что модуль пользователя (12) содержит память модуля (52), в которой функции шифрования и расшифровки (64, 66) обеспечиваются модулем пользователя (12), а также содержатся ключевые данные (60), используемые указанными функциями шифрования и расшифровки (64, 66), причем данные функции шифрования и расшифровки (64, 66) выполняются, по крайней мере, частично процессором (50) модуля пользователя (12).

4. Способ по п.3, отличающийся тем, что, по крайней мере, одна функция генерации (68) ключевых данных (60) и записи ключевых данных (60) в память модуля (52) обеспечивается модулем пользователя (12).

5. Способ по п.1, или 2, или 4, отличающийся тем, что, по крайней мере, выполнение функции расшифровки (66) защищено паролем и/или биометрическим тестом.

6. Способ по п.3, отличающийся тем, что, по крайней мере, выполнение функции расшифровки (66) защищено паролем и/или биометрическим тестом.

7. Способ по любому из пп.1, 2, 4 и 6, отличающийся тем, что мобильное устройство (10) является устройством, настроенным для осуществления телекоммуникационных функций.

8. Способ по п.3, отличающийся тем, что мобильное устройство (10) является устройством, настроенным также для осуществления телекоммуникационных функций.

9. Способ по п.5, отличающийся тем, что мобильное устройство (10) является устройством, настроенным также для осуществления телекоммуникационных функций.

10. Способ по любому из пп.1, 2, 4, 6, 8 и 9, отличающийся тем, что модуль пользователя (12) является модулем идентификации абонента (SIM-картой), предназначенным также для входа в сеть телефонной связи (18).

11. Способ по п.3, отличающийся тем, что модуль пользователя (12) является модулем идентификации абонента (SIM-картой), предназначенным также для входа в сеть телефонной связи (18).

12. Способ по п.5, отличающийся тем, что модуль пользователя (12) является модулем идентификации абонента (SIM-картой), предназначенным также для входа в сеть телефонной связи (18).

13. Способ по п.7, отличающийся тем, что модуль пользователя (12) является модулем идентификации абонента (SIM-картой), предназначенным также для входа в сеть телефонной связи (18).

14. Мобильное устройство (10), в частности мобильный телефон или персональный цифровой помощник, содержащее память (38) и интерфейс (14) для подсоединения модуля пользователя (12), где память (38) содержит, по крайней мере, одну область для хранения пользовательских данных (48) в, по меньшей мере, частично зашифрованном виде, отличающееся тем, что мобильное устройство (10) настроено на использование функции расшифровки (66), по крайней мере, для расшифровки пользовательских данных (48) в операциях доступа, причем функция расшифровки (66) обеспечивается модулем пользователя (12) и, по меньшей мере, частично выполняется процессором (50) модуля пользователя (12).

15. Модуль пользователя (12), в частности модуль идентификации абонента в сети телефонной связи (18), содержащий процессор (50) и настроенный на соединение с мобильным устройством (10), в частности мобильным телефоном или персональным цифровым помощником, через интерфейс (14), причем мобильное устройство (10) содержит память (38), по крайней мере, с одной областью хранения пользовательских данных (48) в, по меньшей мере, частично зашифрованном виде, отличающийся тем, что модуль пользователя (12) настроен на обеспечение мобильного устройства (10) через интерфейс (14) функцией расшифровки (66) для расшифровки, по крайней мере, пользовательских данных (48) в операциях доступа и указанная функция расшифровки (66) выполняется, по крайней мере, частично процессором (50) модуля пользователя (12).

16. Способ хранения и доступа к данным конфигурации (62) и выполнения, по крайней мере, одной программы-приложения (46) в мобильном устройстве (10), в частности в мобильном телефоне или персональном цифровом помощнике, где указанное мобильное устройство (10) содержит память (38) для программы-приложения (46) и подсоединяется через интерфейс (14) к модулю пользователя (12), содержащему память модуля (52), отличающийся тем, что

данные конфигурации (62) связаны, по крайней мере, с доступностью программы-приложения (46) или ее отдельных функций, а также тем, что

данные конфигурации (62) хранятся в памяти модуля (52) и считываются оттуда в целях определения того, можно ли выполнять программу-приложение (46) или в каком объеме ее можно выполнять.

17. Способ по п.16, отличающийся тем, что считывание данных конфигурации (62) из памяти модуля (52) защищено паролем и/или биометрическим тестом.

18. Способ по п.16 или 17, отличающийся тем, что, по крайней мере, части программы-приложения (46) загружаются в память (38) в соответствии с данными конфигурации (62).

19. Способ по п.16 или 17, отличающийся тем, что мобильное устройство (10) является устройством, настроенным также для выполнения телекоммуникационных функций.

20. Способ по п.18, отличающийся тем, что мобильное устройство (10) является устройством, настроенным также для выполнения телекоммуникационных функций.

21. Способ по п.18, отличающийся тем, что, по крайней мере, части программы-приложения (46) передаются в память (38) с помощью как минимум одной телекоммуникационной функции мобильного устройства (10).

22. Способ по п.19, отличающийся тем, что, по крайней мере, части программы-приложения (46) передаются в память (38) с помощью как минимум одной телекоммуникационной функции мобильного устройства (10).

23. Способ по п.20, отличающийся тем, что, по крайней мере, части программы-приложения (46) передаются в память (38) с помощью как минимум одной телекоммуникационной функции мобильного устройства (10).

24. Способ по любому из пп.16, 17, 20-23, отличающийся тем, что модуль пользователя (12) является модулем идентификации абонента (SIM-картой), предназначенный также для входа в сеть телефонной связи (18).

25. Способ по п.18, отличающийся тем, что модуль пользователя (12) является модулем идентификации абонента (SIM-картой), предназначенный также для входа в сеть телефонной связи (18).

26. Способ по п.19, отличающийся тем, что модуль пользователя (12) является модулем идентификации абонента (SIM-картой), предназначенный также для входа в сеть телефонной связи (18).

27. Способ по любому из пп.16, 17, 20-23, 25 и 26, обладающий также признаками способа по любому из пп.1-6.

28. Способ по п.18, обладающий также признаками способа по любому из пп.1-6.

29. Способ по п.19, обладающий также признаками способа по любому из пп.1-6.

30. Способ по п.24, обладающий также признаками способа по любому из пп.1-6.

31. Мобильное устройство (10), в частности мобильный телефон или персональный цифровой помощник, является мобильным устройством (10), содержащим память (38) для программы-приложения (46) и соединяющимся через интерфейс (14) с модулем пользователя (12), содержащим память модуля (52), отличающееся тем, что:

данные конфигурации (62), связанные, по крайней мере, с доступностью программы-приложения (46) или ее отдельных фунцкций, могут считываться из памяти модуля (52) через интерфейс (14), а также тем, что

мобильное устройство (10) настроено таким образом, чтобы определять в зависимости от данных конфгурации (62), считанных из памяти модуля (52), можно ли выполнять программу-приложение (46) или в каком объеме ее можно выполнять.

32. Мобильное устройство (10) по п.31, настроенное также на осуществление во взаимодействии с модулем пользователя (12) способа по любому из пп.16-30.

33. Модуль пользователя (12), в частности модуль идентификации абонента (SIM-карта) для сети телефонной связи (18), содержащий память модуля (52) и настроенный на соединение через интерфейс (14) с мобильным устройством (10), в частности с мобильным телефоном или персональным цифровым помощником, где мобильное устройство (10) содержит память (38) для программы-приложения (46), отличающийся тем, что:

данные конфигурации (62) связаны, по крайней мере, с доступностью программы-приложения (46) или ее отдельных функций, а также тем, что

модуль пользователя (12) настроен на хранение данных конфигурации (62) в памяти модуля (52) и на обеспечение мобильного устройства (10) возможностью считывать данные конфигурации (62) через интерфейс (14) в целях определения того, можно ли выполнять

программу-приложение (46) или в каком объеме ее можно выполнять.