РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 740 298**(13) **C2**

(51) МПК
H04L 9/08 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 21/45 (2020.08); *G06F 21/6209* (2020.08); *G06F 21/6218* (2020.08); *G06F 21/6281* (2020.08); *H04L 9/0861* (2020.08); *H04L 9/088* (2020.08); *H04L 9/30* (2020.08); *H04W 12/0023* (2020.08); *H04W 12/04* (2020.08)

(21)(22) Заявка: **2019116964, 01.12.2017**

(24) Дата начала отсчета срока действия патента:
01.12.2017

Дата регистрации:
13.01.2021

Приоритет(ы):
(30) Конвенционный приоритет:
02.12.2016 GB 1620553.6

(43) Дата публикации заявки: **11.01.2021** Бюл. № 2

(45) Опубликовано: **13.01.2021** Бюл. № 2

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **02.07.2019**

(86) Заявка PCT:
EP 2017/025349 (01.12.2017)

(87) Публикация заявки PCT:
WO 2018/099606 (07.06.2018)

Адрес для переписки:
191036, Санкт-Петербург, а/я 24, "НЕВИНПАТ"

(72) Автор(ы):
КЯРККЯИНЕН Туомас (FI),
КАЛЕВО Осси (FI),
САХЛБОМ Микко (FI)

(73) Патентообладатель(и):
ГУРУЛОДЖИК МИКРОСИСТЕМС ОЙ (FI)

(56) Список документов, цитированных в отчете о поиске: **US 2014/0208100 A1, 24.07.2014. RU 2599538 C2, 10.10.2016. EP 1836640 A2, 26.09.2007. US 9396325 B2, 19.07.2016.**

(54) Защита использования содержимого хранилища ключей

(57) Реферат:

Изобретение относится к системам обеспечения безопасности. Технический результат заключается в обеспечении защиты содержимого хранилища ключей от неавторизованного доступа путем применения завершенного сквозного процесса от поставщика услуг предоставления ключей до данного устройства конечного пользователя. Способ защиты использования содержимого хранилища ключей в устройстве конечного пользователя содержит прием содержимого хранилища ключей, включающего данные ключей, зашифрованные с использованием реквизитов шифрования, совместимых с данным пользовательским устройством, при этом содержимое хранилища ключей создано поставщиком услуг предоставления ключей, импортирование зашифрованных данных ключей содержимого хранилища ключей в защищенное хранилище ключей и сохранение данных ключей, при этом импортируют в ходе выполнения одной операции и внутренне, в защищенном хранилище ключей,

RU 2740298 C2

RU 2740298 C2

предоставление, одной или более интегрированным услугам хранилища ключей данного пользовательского устройства, доступа к неэкспортируемым данным ключей для использования только посредством ссылок на ключи. 3 н. и 15 з.п. ф-лы, 4 ил.

ФИГ. 2

RU 2740298 C2

RU 2740298 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 740 298**(13) **C2**

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

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/45 (2020.08); G06F 21/6209 (2020.08); G06F 21/6218 (2020.08); G06F 21/6281 (2020.08); H04L 9/0861 (2020.08); H04L 9/088 (2020.08); H04L 9/30 (2020.08); H04W 12/0023 (2020.08); H04W 12/04 (2020.08)

(21)(22) Application: **2019116964, 01.12.2017**

(24) Effective date for property rights:
01.12.2017

Registration date:
13.01.2021

Priority:
(30) Convention priority:
02.12.2016 GB 1620553.6

(43) Application published: **11.01.2021** Bull. № 2

(45) Date of publication: **13.01.2021** Bull. № 2

(85) Commencement of national phase: **02.07.2019**

(86) PCT application:
EP 2017/025349 (01.12.2017)

(87) PCT publication:
WO 2018/099606 (07.06.2018)

Mail address:
191036, Sankt-Peterburg, a/ya 24, "NEVINPAT"

(72) Inventor(s):
KARKKAINEN Tuomas (FI),
KALEVO Ossi (FI),
SAHLBOM Mikko (FI)

(73) Proprietor(s):
GURULOGIC MICROSYSTEMS OY (FI)

RU 2740298 C2

(54) PROTECTION OF USAGE OF KEY STORE CONTENT

(57) Abstract:

FIELD: safety system.

SUBSTANCE: method of protecting use of key store content in an end user device comprises receiving key storage content including key data, encrypted using encryption credentials compatible with said user device, wherein the content of the keystore is created by the key service provider, importing encrypted data of key storage content keys into a secure keystore and storing key data, while importing, during one operation and internally, in a secure keystore, providing one or more integrated keys storage services of said user device, accessing non-exported key data for use only by means of links to keys.

EFFECT: technical result consists in protection of key store content from unauthorized access by applying a complete end-to-end process from a key service provider to said end user device.

18 cl, 4 dwg

RU 2740298 C2

ФИГ. 2

RU 2740298 C2

RU 2740298 C2

ОБЛАСТЬ ТЕХНИКИ

Раскрытие настоящего изобретения относится к системам для защиты использования содержимого хранилища ключей (key store) в устройствах конечного пользователя, например, - к системам обеспечения безопасности, в основе которых лежит использование данных ключей (key materials) для реализации защиты данных. Кроме того, раскрытие настоящего изобретения также относится к способам защиты использования содержимого хранилища ключей в устройствах конечных пользователей. Помимо этого, раскрытие настоящего изобретения также относится к компьютерным программным изделиям, содержащим машиночитаемый носитель информации, на котором хранятся машиночитаемые инструкции, исполняемые вычислительным устройством, в состав которого входят аппаратные средства обработки, выполняющие указанные выше способы.

ПРЕДПОСЫЛКИ СОЗДАНИЯ ИЗОБРЕТЕНИЯ

Часто возникает необходимость в хранении на пользовательских устройствах существенных для безопасности пользователя данных, поскольку в настоящий момент доступны различные услуги и функции, разработанные в виде исполняемых программных приложений на пользовательских устройствах, например программных приложений осуществления платежей. В качестве первого примера можно привести множество доступных в настоящее время услуг для выполнения банковских операций и платежей, которым требуются средства обеспечения безопасности для поддержания усиленной защиты клиентов, использующих эти услуги, и предотвращения злонамеренного доступа третьих сторон, пытающихся взломать такие услуги с целью кражи денежных средств. В качестве второго примера можно привести ситуацию, в которой пользователю может потребоваться сохранить секретные или личные ключи для доступа к защищенным сообщениям электронной почты. По этим и многим другим причинам желательно предоставить надежное решение для поддержки хранилища ключей, связанного с данными о ключах.

Существует множество поставщиков услуг обеспечения безопасности, доступных через множество платформ "экосистем", хранилища ключей которых основаны на программном обеспечении. Например, в настоящее время значительное внимание уделяется платформе экосистемы Android™, поскольку во всем мире распространены различные примеры мобильных устройств, таких как планшетные компьютеры, использующие платформу экосистемы Android™. Согласно документам компании Google, система Android™ Keystore хранит криптографические ключи в контейнере, для того чтобы усложнить их извлечение из устройства, совместимого с Android. Система Android™ Keystore - наиболее развитая из всех современных систем хранения ключей в том, что касается обеспечения безопасности, но, к сожалению, в ней все же отсутствуют очень важные функции, требуемые для реализации эффективного решения по защите современных устройств, в большом количестве предлагаемых на рынке. Android™ Keystore предлагает в целом полный набор алгоритмов обеспечения безопасности таких, например, как криптография, генератор ключей, фабрика ключей, генератор пары ключей, mac и подпись. Все эти услуги выполняются внутри аппаратных средств, оснащенных системой хранилища ключей для повышения их эффективности и удобства использования, однако практические требования криптографии не учитываются.

Кроме того, всего лишь за несколько последних лет значительно возросло использование мобильных телефонов, и множество производителей предлагают различные наборы моделей устройств, разработанные на платформе различных экосистем таких, например, как Google® Android™, Apple® iOS™, Microsoft® Windows®

и т.д. С точки зрения обеспечения безопасности возникает проблема, связанная с тем, что в каждой экосистеме реализовано собственное решение по защите существенных для пользователя данных в аппаратном или программном хранилище ключей. Вследствие этого разработчикам приложений очень трудно разобраться с реализациями, относящимся к безопасности, даже теоретически, хотя они известны на базовом уровне. Почти в каждой экосистеме поддерживается собственное решение по реализации хранилища ключей, однако с точки зрения текущих насущных потребностей желательно сфокусироваться на мобильных платформах, поскольку скоро почти каждый человек будет владеть некоторым видом смартфона, оснащенного большим количеством различных приложений, требующих корректно реализованных хранилищ ключей для сохранения существенно важных для безопасности пользователя данных ключей. Теоретически, хранилища ключей решают почти все известные вопросы, относящиеся к безопасности, однако в реальности их программные реализации не удовлетворяют жестким требованиям к аппаратной конструкции однокристальных систем (SoC, System on Chip).

Во-первых, система Android Keystore не разработана для импортирования тысяч или миллионов секретных ключей (а именно, данных ключей), а служит только для поддержки нескольких секретных ключей. Система Android™ Keystore разработана для сценария, в котором одинаковые ключи многократно используются для шифрования. Во-вторых, Android™ Keystore в один момент времени поддерживает импорт только одного обычного исходного ключа, который потенциально не защищен от атак злоумышленников. Это происходит потому, что безопасность Android™ Keystore основана на асимметричном шифровании, очень медленном вычислительном процессе.

Кроме того, существуют общеизвестные программные решения для хранилища ключей, наиболее известным представителем которых является "Bouncy Castle" или "BC". По сравнению с аппаратно реализованной системой Android™ Keystore система BC поддерживает функцию импортирования для защищенных данных ключей в формате описания абстрактного синтаксиса версии один (ASN.1, Abstract Syntax Notation One), которая может безопасно импортировать в хранилище ключей несколько ключей одновременно. Основная проблема, связанная с BC, заключается в том, что данные ключей полностью не защищены от извлечения, поскольку они запрашиваются извне хранилища ключей и предоставляются другому программному приложению, которое затем использует эти данные. Это делает возможным извлечение злоумышленником данных ключей из хранилища ключей при выполнении аутентифицированного запроса. В частности, данные ключей не индексируются в данном хранилище ключей BC, что потенциально делает доступными существенные для безопасности данные ключей для злоумышленников.

В опубликованном документе US 2014/0208100 A1 (H. Richard Kendall; "Provisioning an App on a Device and Implementing a Keystore") описан способ установки хранилища ключей в мобильное приложение. Приложение предлагает пользователю ввести пароль для создания хранилища ключей приложения. Хранилище ключей имеет раздел пользователя и таблицу содержания (Table of Contents, TOC). Файлы в хранилище хэшируют, создавая "первые" значения хэшей хранилища. Эти первые значения хэшей хранилища сохраняют в TOC. TOC хэшируют, создавая значение хэша TOC. Пароль, введенный пользователем, затем комбинируют со значением хэша TOC. Это создает "первый" главный пароль для хранилища ключей. Затем хранилище ключей передают в устройство, где его устанавливают в изолированном приложении общего типа (не поставляемом).

В опубликованном документе (Woo Commerce: "How to Import Serial Keys from CSV file - StoreApps", 21 April 2016 (2016-04-21), XP055461145) дан технический обзор импорта последовательных ключей из файла CSV. Способ включает создание файла CSV, состоящего из текста последовательных ключей, которые должны быть распространены среди пользователей. Созданный файл затем импортируют в панель WooCommerce Serial Key. После импортирования файл CSV проверяют на действительность, и показывают в таблице информацию о том, сколько последовательных ключей импортировано, и какие из них пропущены.

В другом опубликованном документе (Mohamed Sabt et al; "Breaking into the KeyStore: A Practical Forgery Attack Against Android KeyStore") дан технический обзор безопасности хранилища ключей Android KeyStore. Этот документ показывает, что использование схем криптографии с неподтвержденной безопасностью в сложных архитектурах может вызвать серьезные последствия. Документ также показывает, что схема аутентифицированного шифрования (Authenticated Encryption, AE) Hash-then-CBC-Encrypt (хэш-затем-шифрование CBC) не обеспечивает аутентичности, независимо от используемой функции хэширования. Документ также представляет атаку путем избирательной фальсификации, в которой противник использует эту уязвимость, чтобы существенно уменьшить длину симметричных ключей, защищенных хранилищем KeyStore.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

Раскрытие настоящего изобретения направлено на поиск способа реализации усовершенствованной системы для защиты использования содержимого хранилища ключей на устройстве конечного пользователя.

Кроме того, раскрытие настоящего изобретения направлено на поиск усовершенствованного способа защиты использования содержимого хранилища ключей на данном устройстве конечного пользователя.

Другой целью раскрытия настоящего изобретения является по меньшей мере частичное решение по меньшей мере некоторых упомянутых выше проблем, свойственных известному уровню техники.

Согласно первому аспекту посредством вариантов раскрытия настоящего изобретения предлагается способ защиты использования содержимого хранилища ключей в данном устройстве конечного пользователя, включающий следующие шаги:

(i) прием в данном пользовательском устройстве содержимого хранилища ключей, включающего в свой состав данные ключей, зашифрованные с использованием реквизитов (credentials) шифрования, совместимых с данным пользовательским устройством, при этом содержимое хранилища ключей создается поставщиком услуг предоставления ключей и принимается от поставщика услуг предоставления ключей в формате, совместимом с данным пользовательским устройством;

(ii) импортирование зашифрованных данных ключей содержимого хранилища ключей в защищенное хранилище ключей данного пользовательского устройства и сохранение данных ключей в защищенном хранилище ключей в зашифрованном виде, при этом все зашифрованные данные ключей содержимого хранилища ключей импортируются в ходе выполнения одной операции, и содержимое хранилища ключей сохраняется в хранилище ключей таким образом, чтобы данные ключей не экспортировались из хранилища ключей, причем ключи генерируют из зашифрованных данных ключей с использованием:

- смещений ключей,
- смещений битов, и/или

- смещений байтов; и

(iii) внутренне, в защищенном хранилище ключей данного пользовательского устройства предоставление одной или более интегрированным услугам хранилища ключей данного пользовательского устройства доступа к неэкспортируемым данным ключей для использования только посредством ссылок на ключи.

Преимущества настоящего изобретения состоят в том, что полная защита содержимого хранилища ключей от неавторизованного доступа упрощается путем применения завершенного сквозного процесса от поставщика услуг предоставления ключей до данного устройства конечного пользователя, при этом данные ключей содержимого хранилища ключей никогда не раскрываются или не обрабатываются ненадежно на любом шаге процесса, не экспортируются после сохранения в защищенном хранилище ключей данного пользовательского устройства и доступны для использования услугами, интегрированными с защищенным хранилищем ключей, только посредством ссылок на ключи.

Согласно второму аспекту, посредством вариантов раскрытия настоящего изобретения предлагается компьютерное программное изделие, содержащее машиночитаемый носитель информации, на котором хранятся машиночитаемые инструкции, исполняемые вычислительным устройством, в состав которого входят аппаратные средства обработки для выполнения способа, соответствующего вышеуказанному первому аспекту.

Согласно третьему аспекту посредством вариантов раскрытия настоящего изобретения предлагается система для защиты использования содержимого хранилища ключей в данном устройстве конечного пользователя, способная выполнять следующие операции:

(i) прием в данном пользовательском устройстве содержимого хранилища ключей, включающего в свой состав данные ключей, зашифрованные с использованием реквизитов шифрования, совместимых с данным пользовательским устройством, при этом содержимое хранилища ключей создается поставщиком услуг предоставления ключей и принимается от поставщика услуг предоставления ключей в формате, совместимом с данным пользовательским устройством;

(ii) импортирование зашифрованных данных ключей содержимого хранилища ключей в защищенное хранилище ключей данного пользовательского устройства и сохранение данных ключей в защищенном хранилище ключей в зашифрованном виде, при этом все зашифрованные данные ключей содержимого хранилища ключей импортируются в ходе выполнения одной операции, и содержимое хранилища ключей сохраняется в хранилище ключей таким образом, чтобы данные ключей не экспортировались из хранилища ключей, причем ключи генерируют из зашифрованных данных ключей с использованием:

- смещений ключей,
- смещений битов, и/или
- смещений байтов; и

(iii) внутренне, в защищенном хранилище ключей данного пользовательского устройства предоставление одной или более интегрированным услугам хранилища ключей данного пользовательского устройства доступа к неэкспортируемым данным ключей для использования только посредством ссылок на ключи.

Дополнительные аспекты, преимущества, признаки и цели раскрытия настоящего изобретения станут очевидными после ознакомления с чертежами и подробным описанием примеров осуществления, приведенным ниже совместно с прилагаемой

формулой изобретения.

Следует принимать во внимание, что признаки настоящего изобретения допускается комбинировать в различных сочетаниях без нарушения объема изобретения, определенного прилагаемой формулой изобретения.

Предшествующее описание и последующее подробное описание вариантов осуществления настоящего изобретения станут более понятными при их прочтении совместно с прилагаемыми чертежами. С целью иллюстрации настоящего изобретения на чертежах показаны типовые структуры вариантов его осуществления. Однако раскрытие настоящего изобретения не ограничивается конкретными способами и устройствами, раскрываемыми в этом описании. Кроме того, специалисты в данной области техники понимают, что чертежи выполнены не в масштабе. Там, где это возможно, схожие элементы обозначены идентичными номерами.

Варианты осуществления, приведенные в настоящем раскрытии изобретения, описываются ниже только как примеры со ссылкой на прилагаемые чертежи, на которых:

на фиг. 1A показано схематическое представление системы для защиты использования содержимого хранилища ключей в устройстве конечного пользователя в соответствии с вариантом раскрытия настоящего изобретения;

на фиг. 1B показано схематическое представление выполнения операций полного сквозного процесса защиты использования содержимого хранилища ключей в устройстве конечного пользователя в соответствии с вариантом раскрытия настоящего изобретения;

на фиг. 1C показано схематическое представление способа импортирования и загрузки содержимого хранилища ключей в защищенное хранилище ключей пользовательского устройства в соответствии с вариантом раскрытия настоящего изобретения; и

на фиг. 2 показан алгоритм выполнения шагов способа защиты использования содержимого хранилища ключей в устройстве конечного пользователя в соответствии с вариантом раскрытия настоящего изобретения.

На прилагаемых чертежах подчеркнутые числа используются для обозначения элементов, выше которых расположены эти числа, или элементов, рядом с которыми находятся эти числа. Если число не подчеркнуто, но рядом с ним расположена стрелка, то неподчеркнутое число используется для идентификации общего элемента, на который указывает стрелка.

ПОДРОБНОЕ ОПИСАНИЕ ВАРИАНТОВ ОСУЩЕСТВЛЕНИЯ ИЗОБРЕТЕНИЯ

В последующем подробном описании иллюстрируются варианты раскрытия настоящего изобретения и способы их реализации. Хотя в этом описании раскрыты некоторые варианты осуществления настоящего изобретения, специалисты в этой области техники должны понимать, что на практике возможно осуществление других вариантов.

Согласно первому аспекту посредством вариантов раскрытия настоящего изобретения предлагается способ защиты использования содержимого хранилища ключей в устройстве конечного пользователя, включающий следующие шаги:

(i) прием в данном пользовательском устройстве содержимого хранилища ключей, включающего в свой состав данные ключей, зашифрованные с использованием реквизитов шифрования, совместимых с данным пользовательским устройством, при этом содержимое хранилища ключей создается поставщиком услуг предоставления ключей и принимается от поставщика услуг предоставления ключей в формате, совместимом с данным пользовательским устройством;

(ii) импортирование зашифрованных данных ключей содержимого хранилища ключей в защищенное хранилище ключей данного пользовательского устройства и сохранение

данных ключей в защищенном хранилище ключей в зашифрованном виде, при этом все зашифрованные данные ключей содержимого хранилища ключей импортируются в ходе выполнения одной операции, и содержимое хранилища ключей сохраняется в хранилище ключей таким образом, чтобы данные ключей не экспортировались из хранилища ключей, причем ключи генерируют из зашифрованных данных ключей с использованием:

- смещений ключей,
- смещений битов, и/или
- смещений байтов; и

(iii) внутренне, в защищенном хранилище ключей данного пользовательского устройства предоставление одной или более интегрированным услугам хранилища ключей данного пользовательского устройства доступа к неэкспортируемым данным ключей для использования только посредством ссылок на ключи.

Опционально, помимо данных ключей, защищенное хранилище ключей также содержит информацию о конечном пользователе или группе конечных пользователей, авторизованных для применения данных ключей, содержащихся в защищенном хранилище ключей. Дополнительно или в альтернативном варианте, защищенное хранилище ключей содержит другую информацию, относящуюся к использованию данных ключей.

В раскрытии настоящего изобретения термин "конечный пользователь " обозначает как человека, так и машину. Например, конечным пользователем может являться зарегистрированная промежуточная машина. Это может оказаться полезным в тех случаях, когда упомянутый способ используется для распознавания и верификации серверов, которые осуществляют межмашинную связь.

Следует принимать во внимание, что хранилище ключей защищено для его применения только конечным пользователем, то есть защищено от неавторизованного применения другими пользователями, отличными от авторизованного конечного пользователя, и такая защита хранилища ключей не связана с шифрованием импортированных данных ключей. Другими словами, данные ключей шифруются с использованием одного или более различных секретных ключей таких, например, как один или более заранее распределенных ключей.

Опционально, данные ключей принимают на шаге (i) в формате симметричного шифрования. Опционально, в этом отношении данные ключей шифруют с использованием симметричных ключей.

Опционально, способ включает внутреннее, в защищенном хранилище ключей данного пользовательского устройства, дешифрование одного или более набора данных ключей, подлежащего использованию одной или более интегрированными услугами хранилища ключей данного пользовательского устройства.

В раскрытии настоящего изобретения термин "ссылка на ключ " обычно обозначает заданную ссылку, которая указывает и идентифицирует заданные данные ключей, содержащиеся в защищенном хранилище ключей. Другими словами, заданная ссылка на ключ предоставляет сведения о том, какие данные ключей (например, ключ или сертификат) должны использоваться, и опционально, в каком местоположении защищенного хранилища ключей находятся данные ключей, подлежащие использованию.

Согласно вариантам раскрытия настоящего изобретения собственно данные ключей никогда не извлекаются из хранилища ключей.

В соответствии с вариантом осуществления ссылки на ключи реализуются

посредством индексов данных ключей. Опционально, индексы представляют собой порядковые числа данных ключей в порядке их появления. Опционально, способ включает прием, в пределах содержимого хранилища ключей, индексов, используемых для ссылки на данные ключей посредством ссылок на ключи. Опционально, в альтернативном варианте способ включает генерацию в данном пользовательском устройстве индексов, используемых для ссылки на данные ключей посредством ссылок на ключи. Например, индексы могут генерироваться последовательно в соответствии с порядком, в котором данные ключей включаются в содержимое хранилища ключей. Индексы могут генерироваться, например, при начальной регистрации данного пользовательского устройства у поставщика услуг предоставления ключей или в процессе дешифрования данных ключей.

В соответствии с вариантом осуществления, ссылки на ключи реализуются посредством смещений, основанных на том, какие данные ключей должны быть идентифицированы. Следует принимать во внимание, что заданное смещение указывает и идентифицирует заданные данные ключей, содержащиеся в защищенном хранилище ключей. Далее с целью иллюстрации приводятся некоторые примеры смещений.

В соответствии с вариантами раскрытия настоящего изобретения полная защита содержимого хранилища ключей от неавторизованного доступа упрощается путем применения полностью сквозного процесса - от поставщика услуг предоставления ключей до данного устройства конечного пользователя, при этом на любом шаге процесса данные ключей содержимого хранилища ключей никогда не раскрываются или не обрабатываются ненадежно. Содержимое хранилища ключей создается и доставляется в данное пользовательское устройство в зашифрованном виде. Это потенциально предотвращает перехват данных третьей стороной. В данном пользовательском устройстве содержимое хранилища ключей импортируется в хранилище ключей данного пользовательского устройства в ходе выполнения одной операции.

Опционально, содержимое хранилища ключей принимается в виде одного списка, содержащего все данные ключей (далее для удобства называемого "список кодов ключей"). Опционально, в альтернативном варианте содержимое хранилища ключей принимается в виде множества списков кодов ключей. Следует принимать во внимание, что множество списков кодов ключей может импортироваться одновременно. Независимо от формата, в котором зашифрованы различные списки кодов ключей, то есть данные ключей, все данные ключей импортируются в ходе выполнения одной операции.

Опционально, на шаге (ii) содержимое хранилища ключей импортируется в данное пользовательское устройство в виде одного файла данных. Следует принимать во внимание, что количество наборов данных ключей, включенных в содержимое хранилища ключей, может превышать тысячи, а потенциально миллионы. В таком случае импортирование содержимого хранилища ключей в виде одного файла данных обладает несколькими преимуществами по сравнению с традиционными способами хранения ключей.

Далее, только с целью иллюстрации, рассматривается пример реализации упомянутой выше системы с использованием продукта "Starwindow®", разработанного компанией Gurulogic Microsystem Oy. В такой реализации после приема содержимого хранилища ключей в данном пользовательском устройстве для импортирования всех данных ключей в хранилище ключей в ходе выполнения одной операции используется функция "Load" (загрузка), предоставляемая продуктом "Starwindow®". Кроме того, функция

"Load" выполняет безопасное дешифрование данных ключей в хранилище ключей для обеспечения их быстрого использования. Следует принимать во внимание, что функция "Load" может использоваться для импортирования всех данных ключей в ходе выполнения одной операции, даже если в содержимое хранилища ключей включены миллионы наборов данных ключей.

Указанное выше одновременное импортирование значительного объема данных ключей может быть реализовано различными способами, например, с помощью приведенных ниже вариантов реализации.

Вариант A

Список кодов ключей содержит восемь различных 128-битовых ключей, и этот список кодов ключей занимает в памяти пространство размером в 128 байт. Поскольку наименьшей единицей измерения является один байт, равный восьми битам, то 128-битовый ключ занимает в памяти 16 байт. Следует принимать во внимание, что ключи обычно представляют максимально возможную энтропию, что повышает достигаемый в результате уровень защиты, и, таким образом, эти ключи не могут быть сжаты с помощью традиционных способов сжатия.

Например, список кодов ключей может быть представлен следующим образом:

KeyCodeListA: array [0..7] of array [0..15] of UInt8=

(0x4B, 0xDA, 0x72, 0x44, 0xBЗ, 0x12, 0x07, 0x43, 0x6F, 0x65, 0x83, 0x8C, 0xF5, 0x3F, 0xF1, 0x08, //ключ 1

0xCA, 0x1E, 0x7F, 0xDF, 0x5C, 0x7F, 0x78, 0x0C, 0x55, 0x88, 0x96, 0x0B, 0xA9, 0xD9, 0x22, 0x6F, //ключ 2

0xBб, 0x43, 0x73, 0x84, 0x57, 0x86, 0x66, 0xF8, 0x79, 0xB0, 0xCC, 0xA0, 0x16, 0x13, 0x42, 0xDF, //ключ 3

0xF0, 0xбB, 0x2B, 0xF8, 0x68, 0x5A, 0x31, 0xCF, 0x9A, 0x65, 0xF1, 0xC7, 0x94, 0x62, 0xDD, 0x9 B, //ключ 4

0xB1, 0x28, 0x68, 0xEE, 0x1B, 0x4D, 0x43, 0x07, 0xE4, 0x97, 1xFF, 0x00, 0x01, 0xFF, 0x00, 0xE0, //ключ 5

0xEE, 0x1F, 0xFD, 0xA9, 0x69, 0xE5, 0xFF, 0x00, 0xDF, 0x67, 0x67, 0xF7 0xB0, 0xB9, 0xAA, 0x77, //ключ 6

0x9E, 0x55, 0xAC, 0xEЗ, 0xFE, 0x16, 0x27, 0xD9, 0xED, 0xE1, 0x2B, 0xFF 0x00, 0x13, 0xFF, 0x00, //ключ 7

0xB5, 0xE2, 0x28, 0x56, 0x2D, 0xBF, 0xE9, 0x39, 0x1F, 0xF0, 0x74, 0x9F, 0x95, 0x19, 0x05, 0x07, //ключ 8);

где каждая из последовательностей, состоящих из 16 байт, представляет собой ключ. В этом примере ключи генерируются на основе смещений ключей, то есть путем увеличения смещений на размер ключа (составляющий в этом примере 16 байт).

Опционально, импортирование в ходе выполнения одной операции осуществляется путем "сжатия" ключей, подлежащих доставке. Для реализации этого существуют по меньшей мере два различных способа, а именно: варианты 1) "B" и "C", и 2) "D".

Вариант B

С целью иллюстрации вариант "B" далее описывается на основе того же примера списка кодов ключей. Опционально, 128 ключей (=8x16) генерируются из того же списка кодов ключей путем выбора ключей на основе смещений байтов, а не смещений ключей. Например, первые три ключа могут генерироваться следующим образом:

KeyCodeListB: array [0..127] of UInt8=

(0x4 B, 0xDA, 0x72, 0x44, 0xBЗ, 0x12, 0x07, 0x43, 0x6F, 0x65, 0x83, 0x8C, 0xF5, 0x3F, 0xF1, 0x08, // ключ 1 с байтовым смещением "0"

(0xDA, 0x72, 0x44, 0xB3, 0x12, 0x07, 0x43, 0x6F, 0x65, 0x83, 0x8C, 0xF5, 0x3F, 0xF1, 0x08, 0xCA // ключ 2 с байтовым смещением "1" (0x72, 0x44, 0xB3, 0x12, 0x07, 0x43, 0x6F, 0x65, 0x83, 0x8C, 0xF5, 0x3F, 0xF1, 0x08, 0xCA, 0x1E, // ключ 3 с байтовым смещением "2"

Следует принимать во внимание, что ключи могут генерироваться путем выбора смещения в любом предварительно определенном порядке, и ключи не обязательно всегда генерируются путем увеличения смещения на единицу, как показано в представленном выше примере для списка кодов ключей, приведенного в варианте "A".

Вариант C

С помощью того же списка кодов ключей можно сгенерировать 1024 ключа (=8x16x8 ключей), а не указанные выше восемь (8) и 128 ключей, путем выбора ключей на основе битового смещения, а не смещения ключей или байтов. Например, первые три 16-байтовых ключа (сгенерированных в варианте "B") могут быть преобразованы в биты следующим образом:

0100 1011 1101 1010 0111 0010 0100 0100 1011 0011 0001 0010 0000 0111 0100 0011 0110 1111 0110 0101 1000 0011 1000 1100 1111 0101 0011 1111 1111 0001 0000 1000 1101 1010 0111 0010 0100 0100 1011 0011 0001 0010 0000 0111 0100 0011 0110 1111 0110 0101 1000 0011 1000 1100 1111 0101 0011 1111 1111 0001 0000 1000 1100 1010 0111 0010 0100 0100 1011 0011 0001 0010 0000 0111 0100 0011 0110 1111 0110 0101

1000 0011 1000 1100 1111 0101 0011 1111 1111 0001 0000 1000 1100 1010 0001 1110 Таким образом, первый 128-битовый ключ с битовым смещением "0" выглядит следующим образом:

0100 1011 1101 1010 0111 0010 0100 0100 1011 0011 0001 0010 0000 0111 0100 0011 0110 1111 0110 0101 1000 0011 1000 1100 1111 0101 0011 1111 1111 0001 0000 1000 второй 128-битовый ключ с битовым смещением "1" выглядит следующим образом:

1001 0111 1011 0100 1110 0100 1000 1001 0110 0110 0010 0100 0000 1110 1000 0110 1101 1110 1100 1011 0000 0111 0001 1001 1110 1010 0111 1111 11100010 0001 0001 и третий 128-битовый ключ с битовым смещением "2" выглядит следующим образом:

0010 1111 0110 1001 1100 1001 0001 0010 1100 1100 0100 1000 0001 1101 0000 1101 1011 1101 1001 01100000 11100011 0011 1101 0100 1111 1111 11000100 00100011 Другими словами, по сравнению с исходными ключами этот способ позволяет сгенерировать в 128 раз больше ключей с использованием того же объема данных ключей.

Следует принимать во внимание, что вместо использования указанного выше смещения ключа, байтового смещения или битового смещения также могут использоваться другие типы смещения, например смещение на величину слова, в зависимости от того, какой из факторов более существенен: скорость обработки или увеличение количества сгенерированных ключей.

Вариант D

В соответствии с вариантом осуществления 65535 ключей расширяются в памяти данного пользовательского устройства, например, следующим образом:

(a) 128-битовый ключ расширяется, например, до 352-битового ключа;

(b) 192-битовый ключ расширяется, например, до 432-битового ключа; и

(c) 256-битовый ключ расширяется, например, до 512-битового ключа.

Эти ключи затем могут использоваться с учетом услуг, интегрированных в хранилище ключей, например, с использованием таких алгоритмов, как AES, Salsa20 и ChaCha20, без ограничения приведенными примерами.

Данные ключей могут использоваться в различных целях, например, для

криптографии, защиты данных (например, шифрования и дешифрования), подписи, проверки целостности, верификации, аутентификации, авторизации и т.п. Данные ключей становятся доступными для использования внутренне, в пределах защищенного хранилища ключей, интегрированным в хранилище ключей услугам, которые осуществляют доступ к данным ключей только с помощью ссылок на ключи. Другими словами, данные ключей не доступны программным приложениям или процессам экосистемы извне хранилища ключей.

В том случае, если злоумышленник осуществляет попытку использовать ссылку на ключ для доступа, анализа или отладки соответствующих данных ключей, например, генерируется исключение. Например, если хранилище ключей реализовано на платформе Android™ и технические интерфейсы встроены с использованием Java, где техническая реализация решений по обеспечению безопасности распределяется между Sun Microsystem® Java и Google Android™ Java, то хранилище ключей должно в точности поддерживать требуемые интерфейсы, определенные в рекомендациях разработчика Google Android™, для того чтобы техническая реализация могла быть выполнена с помощью уже существующего прикладного программного интерфейса (API, Application Programming Interface) Java. Однако техническая реализация хранилища ключей не позволяет выполнять доступ, анализ или отладку данных ключей, указываемых посредством заданной ссылки на ключ.

Согласно вариантам раскрытия настоящего изобретения содержимое хранилища ключей создается поставщиком услуг предоставления ключей в указанном выше формате, то есть в формате, совместимом с данным пользовательским устройством, для поддержки совместимости с функцией импортирования хранилища ключей данного пользовательского устройства. Это существенно ускоряет выполнение процедуры импортирования на шаге (ii) в данном пользовательском устройстве. Опционально, содержимое хранилища ключей создается поставщиком услуг предоставления ключей в формате, совместимом с функцией импортирования хранилища ключей для широкого спектра пользовательских устройств; например, пользовательские устройства применяют различные типы внутренних защищенных хранилищ ключей, таких как упомянутая ниже среда TEE, а также применяют переносимые программные интерфейсы для обеспечения переноса стандартных функций, предоставляемых защищенным хранилищем ключей для принимаемого зашифрованного файла содержимого хранилища ключей, переданного поставщиком услуг предоставления ключей. Опционально, в этом отношении на стороне поставщика услуг предоставления ключей отдельно настраивается содержимое хранилища ключей для совместимости с различными типами пользовательских устройств.

Примеры таких пользовательских устройств включают, без ограничения указанными устройствами, мобильные телефоны, смартфоны, мобильные Интернет-устройства (MID, Mobile Internet Device), планшетные компьютеры, ультра-мобильные персональные компьютеры (UMPC, Ultra-Mobile Personal Computer), компьютеры, сочетающие функции смартфона и планшета, персональные информационные устройства (PDA, Personal Digital Assistant), веб-блокноты, персональные компьютеры (PC, Personal Computer), портативные PC, ноутбуки, настольные компьютеры и интерактивные развлекательные устройства, такие как игровые консоли, телевизионные приемники (TV) и телевизионные приставки (STB, Set-Top Box).

Кроме того, следует принимать во внимание, что хранилище ключей пользовательского устройства может быть реализовано либо аппаратно, либо программно, например, с использованием аппаратных средств, таких как TEE ("trusted

execution environment", доверенная среда выполнения), которые предотвращают экспорт из них данных после начального импортирования и загрузки содержимого хранилища ключей в защищенное хранилище ключей данного пользовательского устройства.

В соответствии с вариантом раскрытия настоящего изобретения, хранилище ключей реализовано аппаратно. Опционально, в этом случае импортирование на шаге (ii) включает связывание данных ключей, содержащихся в аппаратном хранилище ключей, с защищенной областью аппаратных средств обработки данного пользовательского устройства. Впоследствии, при использовании, данные ключей, содержащиеся в аппаратном хранилище ключей, становятся доступными посредством ссылок на них, но не могут экспортироваться из хранилища ключей. Опционально, для передачи ссылки на ключ в данных ключей, подлежащих использованию интегрированной услугой хранилища ключей, используется указатель.

Одно или более доверенных программных приложений, например алгоритмы шифрования и/или дешифрования, требующие использования данных ключей в хранилище ключей, защищены в процессе функционирования на уровне ядра данного пользовательского устройства. Уровень ядра данного пользовательского устройства, например, реализуется в виде совокупности аппаратных и программных средств и часто является собственным для данного пользовательского устройства, например, для его изготовителя. Интерфейс доверенных программных приложений с другими программными приложениями, поддерживаемыми на других уровнях программного обеспечения, обеспечивается в процессе функционирования на данном пользовательском устройстве. Одно или более доверенных программных приложений загружаются в зашифрованном виде от поставщика услуг предоставления доверенного программного обеспечения. Опционально, услуги предоставления ключей и доверенного программного обеспечения могут обеспечиваться одним поставщиком. В альтернативном варианте услуги предоставления ключей и доверенного программного обеспечения могут обеспечиваться различными поставщиками.

Таким образом, следует принимать во внимание, что в пользовательском устройстве, содержащем аппаратно реализованное хранилище ключей, существует также уровень ядра и один или более уровней программного обеспечения, размещенных в этом устройстве. Программные приложения могут импортироваться, а затем выполняться на одном или более уровнях программного обеспечения. Кроме того, на уровне ядра могут выполняться другие доверенные программные приложения, обеспечиваемые поставщиком услуг предоставления доверенного программного обеспечения, и в этом случае доверенные программные приложения защищаются средствами обеспечения безопасности уровня ядра, которые обычно более надежны, чем один или более уровней программного обеспечения; при этом программные приложения, защищенные средствами обеспечения безопасности уровня ядра, в рамках раскрытия настоящего изобретения называются "интегрированными услугами хранилища ключей". В процессе функционирования осуществляется обмен различными данными между приложениями, поддерживаемыми на одном или более уровнях программного обеспечения, и "интегрированными услугами хранилища ключей", размещенными на уровне ядра.

Опционально, защищенная область аппаратных средств обработки реализуется посредством специализированной аппаратуры, сконфигурированной для запрета функционирования внешним загруженным программным приложениям или программам, а именно: программам одного или более упомянутых выше уровней программного обеспечения. Следует принимать во внимание, что такие внешние загруженные программные приложения или программы могут намеренно загружаться

злоумышленниками. Более конкретно, защищенная область аппаратных средств обработки, например, реализуется посредством доверенной среды выполнения (TEE; см. ссылку [1]), как указано выше.

Таким образом, способ упрощает устойчивую и надежную интеграцию между программным обеспечением и аппаратурой обеспечения безопасности данного пользовательского устройства.

В соответствии с вариантом раскрытия настоящего изобретения в состав данных ключей входит по меньшей мере одно из следующего:

(a) секретные ключи для симметричного шифрования данных,

(b) личные ключи и открытые ключи для использования в инфраструктуре, эквивалентной инфраструктуре открытых ключей (PKI, Public Key Infrastructure),

(c) сертификаты, подлежащие использованию для криптографии, подписания, обеспечения целостности, верификации, аутентификации, авторизации и т.п.,

(d) один или более генераторов для генерации ключей.

Опционально, в этом отношении один или более генераторов ключей используется для воспроизводимой генерации ключей. Другими словами, каждый раз при использовании одинаковых входных данных заданным генератором ключей генерируется одинаковый ключ.

Опционально, один или более наборов данных ключей индивидуально защищается посредством дополнительного шифрования. В частности, это полезно для определенных приложений обеспечения безопасности.

Следует принимать во внимание, что даже если PKI таким образом использует асимметричное шифрование, данные ключей по-прежнему могут импортироваться с использованием симметричного шифрования.

Кроме того, данные ключей содержат одноразовые ключи, используемые однократно и подлежащие уничтожению после применения. Такие одноразовые ключи могут, например, использоваться для подписки на заданную услугу. Дополнительно или в альтернативном варианте, по меньшей мере некоторые из ключей представляют собой повторно используемые ключи шифрования.

Кроме того, хранилище ключей способно действовать в качестве генератора ключей и генерировать новые воспроизводимые ключи.

Помимо этого, в соответствии с вариантами раскрытия настоящего изобретения способ включает интеграцию с хранилищем ключей одного или более доверенных программных приложений или процессов экосистем, выполняющихся и авторизованных для применения хранилища ключей в данном пользовательском устройстве. Такие интегрированные программные приложения или процессы экосистем в раскрытии настоящего изобретения называются "интегрированными услугами хранилища ключей", как было указано выше. Примеры интегрированных услуг хранилища ключей без ограничения включают услуги доставки данных, услуги доставки содержимого, банковские услуги и услуги финансовых транзакций, в которых обычно задействовано шифрование и/или дешифрование данных с использованием одного или более ключей.

Опционально, в этом отношении способ включает импортирование от поставщика услуг предоставления доверенного программного обеспечения одного или более доверенных программных приложений для предоставления интегрированных услуг хранилища ключей, при этом одно или более доверенных программных приложений при выполнении на данном пользовательском устройстве способны предоставлять одну или более интегрированных услуг хранилища ключей и защищены на уровне ядра данного пользовательского устройства.

Кроме того, если хранилище ключей реализовано аппаратно, данные ключей шифруются с использованием симметричного шифрования, совместимого с аппаратным хранилищем ключей. Опционально, в этом отношении способ включает шифрование данных ключей на стороне поставщика услуг предоставления ключей путем применения усовершенствованного стандарта симметричного шифрования (AES, Advanced Encryption Standard; см. ссылку [2]), например, путем применения 128-битового или 256-битового ключа.

В альтернативном варианте, если хранилище ключей реализовано программно, содержимое хранилища ключей шифруется с использованием асимметричного шифрования, совместимого с программным хранилищем ключей.

Следует принимать во внимание, что для дешифрования зашифрованного содержимого хранилища ключей данному пользовательскому устройству должны быть известны реквизиты, используемые в процессе шифрования. Следует принимать во внимание, что в варианте раскрытия настоящего изобретения не существенно, какой алгоритм шифрования или какие реквизиты шифрования используются для шифрования содержимого хранилища ключей, поскольку различные производители устройств и поставщики экосистем могут реализовывать множество различных решений по обеспечению безопасности, которые затем могут осуществляться множеством различных поставщиков услуг обеспечения безопасности на различных платформах с помощью собственных аппаратных или программных хранилищ ключей.

Кроме того, как указывалось выше, реквизиты шифрования, используемые для шифрования данных ключей, совместимы с данным пользовательским устройством. Такие совместимые реквизиты шифрования могут предоставляться данным пользовательским устройством или поставщиком услуг предоставления ключей. Опционально, в этом отношении способ включает шифрование содержимого хранилища ключей на стороне поставщика услуг предоставления ключей с помощью ключей шифрования, предоставляемых данным пользовательским устройством или поставщиком услуг предоставления ключей.

В соответствии с вариантом раскрытия настоящего изобретения способ включает защиту хранилища ключей в данном пользовательском устройстве с помощью биологического идентификационного удостоверения конечного пользователя. Опционально, в этом отношении биологическое идентификационное удостоверение конечного пользователя представляет собой одно из следующего: отпечаток пальца конечного пользователя, характеристики лица конечного пользователя, профиль ДНК конечного пользователя, радужная оболочка глаза конечного пользователя, походка конечного пользователя, почерк конечного пользователя, образец сердечного ритма конечного пользователя. Следует принимать во внимание, что биологические характеристики конечного пользователя, применяемые для защиты хранилища ключей, предоставляются посредством аппаратных функций устройства конечного пользователя. Эти аппаратные функции, например, могут быть реализованы посредством TEE. Например, характеристики лица конечного пользователя могут распознаваться с помощью камеры устройства конечного пользователя и сравниваться с эталонным шаблоном посредством корреляции изображений или алгоритмов нейронных сетей. Следует принимать во внимание, что биологические характеристики конечного пользователя в альтернативном варианте могут соответствовать любому другому типу биометрической верификации, осуществимой в будущем.

В соответствии с другим вариантом раскрытия настоящего изобретения способ включает защиту хранилища ключей в данном пользовательском устройстве с помощью

персонального идентификационного кода (PIN, Personal Identification Code), связанного с конечным пользователем. Следует принимать во внимание, что PIN предоставляется посредством аппаратных функций устройства конечного пользователя.

В соответствии с еще одним вариантом раскрытия настоящего изобретения способ включает защиту хранилища ключей в данном пользовательском устройстве с помощью специфичного для приложения идентификатора. Опционально, специфичный для приложения идентификатор предоставляется посредством аппаратных функций устройства конечного пользователя. В альтернативном варианте специфичный для приложения идентификатор предоставляется посредством функций, основанных на платформе. Опционально, в этом случае специфичный для приложения идентификатор является идентификатором экземпляра приложения.

Кроме того, в соответствии с вариантом раскрытия настоящего изобретения содержимое хранилища ключей принимается на шаге (i) с помощью незащищенной доставки. Например, зашифрованное содержимое хранилища ключей может передаваться по незащищенному общедоступному Интернет-соединению, поскольку должным образом защищенное и зашифрованное содержимое хранилища ключей не раскрывает каких-либо существенных для пользователя данных. Это возможно, поскольку данные ключей защищены с помощью шифрования, и, таким образом, доставка данных ключей не обязательно должна осуществляться в защищенном режиме.

Согласно второму аспекту посредством вариантов раскрытия настоящего изобретения предлагается компьютерное программное изделие, содержащее машиночитаемый носитель информации, на котором хранятся машиночитаемые инструкции, исполняемые вычислительным устройством, в состав которого входят аппаратные средства обработки для выполнения способа, соответствующего вышеуказанному первому аспекту.

Опционально, машиночитаемые инструкции могут загружаться в вычислительное устройство из хранилища программных приложений, например, из Интернет-магазина "App store".

Согласно третьему аспекту посредством вариантов раскрытия настоящего изобретения предлагается система для защиты использования содержимого хранилища ключей в данном устройстве конечного пользователя, способная выполнять следующие операции:

(i) прием в данном пользовательском устройстве содержимого хранилища ключей, включающего в свой состав данные ключей, зашифрованные с использованием реквизитов шифрования, совместимых с данным пользовательским устройством, при этом содержимое хранилища ключей создается поставщиком услуг предоставления ключей и принимается от поставщика услуг предоставления ключей в формате, совместимом с данным пользовательским устройством;

(ii) импортирование зашифрованных данных ключей содержимого хранилища ключей в защищенное хранилище ключей данного пользовательского устройства и сохранение данных ключей в защищенном хранилище ключей в зашифрованном виде, при этом все зашифрованные данные ключей содержимого хранилища ключей импортируются в ходе выполнения одной операции, и содержимое хранилища ключей сохраняется в хранилище ключей таким образом, чтобы данные ключей не экспортировались из хранилища ключей, причем ключи генерируют из зашифрованных данных ключей с использованием:

- смещений ключей,
- смещений битов, и/или

- смещений байтов; и

(iii) внутренне, в защищенном хранилище ключей данного пользовательского устройства, предоставление одной или более интегрированным услугам хранилища ключей данного пользовательского устройства доступа к неэкспортируемым данным ключей для использования только посредством ссылок на ключи.

Опционально, помимо данных ключей, защищенное хранилище ключей также содержит информацию о конечном пользователе или группе конечных пользователей, авторизованных для применения данных ключей, содержащихся в защищенном хранилище ключей. Дополнительно или в альтернативном варианте, защищенное хранилище ключей содержит другую информацию, относящуюся к использованию данных ключей.

Опционально, данные ключей принимаются на шаге (i) в формате симметричного шифрования.

Опционально, система способна внутренне, в защищенном хранилище ключей данного пользовательского устройства, дешифровать один или более наборов данных ключей, подлежащих использованию одной или более интегрированными услугами данного пользовательского устройства.

В соответствии с вариантом осуществления ссылки на ключи реализуются посредством индексов данных ключей. Опционально, система способна принимать, в пределах содержимого хранилища ключей, индексы, используемые для ссылки на данные ключей посредством ссылок на ключи. Опционально, в альтернативном варианте система способна генерировать в данном пользовательском устройстве индексы, используемые для ссылки на данные ключей посредством ссылок на ключи. Например, индексы могут генерироваться последовательно в соответствии с порядком, в котором данные ключей включаются в содержимое хранилища ключей. Индексы могут генерироваться, например, при начальной регистрации данного пользовательского устройства у поставщика услуг предоставления ключей или в процессе дешифрования данных ключей.

В соответствии с вариантом осуществления ссылки на ключи реализуются посредством смещений, основанных на том, какие данные ключей должны быть идентифицированы.

Опционально, при импортировании на шаге (ii) система способна импортировать содержимое хранилища ключей в данное пользовательское устройство в виде одного файла данных.

Следует принимать во внимание, что варианты раскрытия настоящего изобретения применимы для различных типов пользовательских устройств. Примеры таких пользовательских устройств включают, без ограничения указанными устройствами, мобильные телефоны, смартфоны, MID, планшетные компьютеры, UMPC, компьютеры, сочетающие функции смартфона и планшета, PDA, веб-блокноты, PC, портативные PC, ноутбуки, настольные компьютеры и интерактивные развлекательные устройства, такие как игровые консоли, телевизионные приемники и STB.

В соответствии с вариантом раскрытия настоящего изобретения хранилище ключей реализовано аппаратно. Опционально, в этом случае при импортировании на шаге (ii) система способна связывать данные ключей, содержащихся в аппаратном хранилище ключей, с защищенной областью аппаратных средств обработки данного пользовательского устройства.

Опционально, защищенная область аппаратных средств обработки реализуется с помощью специализированной аппаратуры, сконфигурированной для запрета

функционирования на специализированной аппаратуре внешним загруженным программным приложениям или программам, например, программные приложения, загруженные извне, способны взаимодействовать через интегрированные услуги хранилища ключей, предоставляемые доверенными программными приложениями, которые защищены уровнем ядра устройства конечного пользователя, при этом интегрированные услуги хранилища ключей защищают хранилище ключей от попыток непосредственного доступа, осуществляемых внешними загруженными программными приложениями. Следует принимать во внимание, что такие внешние загруженные программные приложения или программы могут намеренно загружаться злоумышленниками. Однако следует принимать во внимание, что интегрированные услуги хранилища ключей реализуются с использованием доверенных программных приложений, обеспечиваемых поставщиком услуг предоставления доверенного программного обеспечения, как указывалось выше. Более конкретно, защищенная область аппаратных средств обработки реализуется посредством TEE (см. ссылку [1]).

В соответствии с вариантом раскрытия настоящего изобретения в состав данных ключей входит по меньшей мере одно из следующего:

(a) секретные ключи для симметричного шифрования данных,

(b) личные ключи и открытые ключи для использования в инфраструктуре, эквивалентной PKI,

(c) сертификаты, подлежащие использованию для криптографии, подписания, обеспечения целостности, верификации, аутентификации, авторизации и т.п.,

(d) один или более генераторов для генерации ключей.

Помимо этого, в соответствии с вариантом раскрытия настоящего изобретения система способна интегрировать с использованием хранилища ключей одно или более доверенных программных приложений или процессов экосистем, выполняющихся и авторизованных для применения хранилища ключей в данном пользовательском устройстве. Примеры таких интегрированных услуг хранилища ключей без ограничения включают услуги доставки данных, услуги доставки содержимого, банковские услуги и услуги финансовых транзакций.

Опционально, в этом отношении система способна импортировать от поставщика услуг предоставления доверенного программного обеспечения одно или более доверенных программных приложений для предоставления интегрированных услуг хранилища ключей, при этом одно или более доверенных программных приложений при выполнении на данном пользовательском устройстве способны предоставлять одну или более интегрированных услуг хранилища ключей и защищены на уровне ядра данного пользовательского устройства.

Кроме того, в соответствии с вариантом раскрытия настоящего изобретения поставщик услуг предоставления ключей способен шифровать содержимое хранилища ключей с помощью ключей шифрования, предоставляемых данным пользовательским устройством или поставщиком услуг предоставления ключей.

В соответствии с вариантом раскрытия настоящего изобретения хранилище ключей защищено в данном пользовательском устройстве с помощью биологического идентификационного удостоверения конечного пользователя. Опционально, в этом отношении биологическое идентификационное удостоверение конечного пользователя представляет собой одно из следующего: отпечаток пальца конечного пользователя, характеристики лица конечного пользователя, профиль ДНК конечного пользователя, радужная оболочка глаза конечного пользователя, походка конечного пользователя,

почерк конечного пользователя, образец сердечного ритма конечного пользователя. Следует принимать во внимание, что биологические характеристики конечного пользователя в альтернативном варианте могут соответствовать любому другому типу биометрической верификации, осуществимой в будущем.

В соответствии с другим вариантом раскрытия настоящего изобретения хранилище ключей защищено в данном пользовательском устройстве с помощью PIN-кода, связанного с конечным пользователем.

В соответствии с еще одним вариантом раскрытия настоящего изобретения хранилище ключей защищено в данном пользовательском устройстве с помощью специфичного для приложения идентификатора.

Опционально, поставщик услуг предоставления ключей способен шифровать данные ключей путем применения симметричного шифрования AES (см. ссылку [2]), например, с помощью 128-битового или 256-битового ключа.

Кроме того, в соответствии с вариантом раскрытия настоящего изобретения в процессе приема на шаге (i) система способна принимать содержимое хранилища ключей с помощью незащищенной доставки.

Далее со ссылкой на чертежи описываются варианты раскрытия настоящего изобретения.

На фиг. 1 показано схематическое представление системы 100 защиты использования содержимого 102 хранилища ключей в соответствии с вариантом раскрытия настоящего изобретения. Система 100 содержит поставщика 104 услуг предоставления ключей и устройство 106 конечного пользователя, при этом поставщик 104 услуг предоставления ключей и данное устройство 106 конечного пользователя связаны в процессе работы через структуру обмена данными.

Поставщик 104 услуг предоставления ключей создает содержимое 102 хранилища ключей в формате, совместимом с данным устройством 106 конечного пользователя, шифрует данные ключей, включаемые в содержимое 102 хранилища ключей, и передает содержимое 102 хранилища ключей в данное устройство 106 конечного пользователя. Опционально, содержимое 102 хранилища ключей может в виде одного файла импортироваться в защищенное хранилище 108 ключей данного устройства 106 конечного пользователя.

В данном пользовательском устройстве 106 содержимое 102 хранилища ключей (то есть, все данные ключей) импортируется в защищенное хранилище 108 ключей данного пользовательского устройства 106 в ходе выполнения одной операции, при этом данные ключей сохраняются в зашифрованном виде таким образом, чтобы они не экспортировались из защищенного хранилища 108 ключей и были доступны интегрированным услугам хранилища ключей только с помощью ссылок на ключи.

Как описывалось ранее, ссылки на ключи могут быть реализованы посредством индексов или смещений. Опционально, индексы принимаются в содержимом 102 хранилища ключей; в альтернативном варианте индексы генерируются в данном пользовательском устройстве 106, например, последовательно в порядке, в котором данные ключей включаются в содержимое 102 хранилища ключей.

Поставщик 120 услуг предоставления доверенного программного обеспечения предоставляет одно или более доверенных программных приложений 122, импортируемых в зашифрованном виде в защищенное хранилище 108 ключей данного пользовательского устройства 106, при этом одно или более доверенных программных приложений 122 выполняются под управлением данного пользовательского устройства 106 в режиме защиты ядром 124, например уровнем ядра, данного пользовательского

устройства 106. Одно или более доверенных программных приложений 122 способны с различными целями использовать ссылки на ключи для доступа к данным ключей хранилища 108 ключей, например, для шифрования, дешифрования, верификации, аутентификации, однако эти приложения защищены от раскрытия данных ключей другим программным приложениям, поддерживаемым на одном или более уровнях программного обеспечения данного пользовательского устройства 106. Поскольку данные ключей хранятся в зашифрованном виде, их требуется расшифровать перед использованием. Опционально, зашифрованные данные ключей безопасно дешифруются в хранилище 108 ключей при их загрузке в хранилище 108 ключей.

Опционально, поставщик 120 услуг предоставления доверенного программного обеспечения и поставщик 104 услуг предоставления ключей может представлять собой одну и ту же сторону. В альтернативном варианте поставщик 120 услуг предоставления доверенного программного обеспечения отличается от поставщика 104 услуг предоставления ключей.

На фиг. 1B показано схематическое представление выполнения операций полного сквозного процесса защиты использования содержимого 102 хранилища ключей на данном устройстве 106 конечного пользователя в соответствии с вариантом раскрытия настоящего изобретения.

Шаг 1: поставщик 104 услуг предоставления ключей создает содержимое 102 хранилища ключей в формате, совместимом с данным пользовательским устройством 106.

Шаг 2: поставщик 104 услуг предоставления ключей шифрует данные ключей, включаемые в содержимое 102 хранилища ключей.

Шаг 3: данное пользовательское устройство 106 принимает содержимое 102 хранилища ключей от поставщика 104 услуг предоставления ключей.

Шаг 4: зашифрованные данные ключей импортируются в защищенное хранилище 108 ключей данного пользовательского устройства 106. Опционально, хранилище 108 ключей защищается с использованием реквизитов шифрования конечного пользователя.

Шаг 5: данные ключей загружаются в хранилище ключей, при этом данные ключей дешифруются в безопасном режиме в хранилище ключей для обеспечения простого и быстрого их использования.

Шаг 6: интегрированные услуги 122 хранилища ключей внутренне осуществляют доступ к данным ключей в пределах защищенного хранилища ключей только с помощью ссылок на ключи.

Запрещенный шаг 7: данные ключей не могут экспортироваться из хранилища 108 ключей.

Кроме того, на фиг. 1C показано схематическое представление способа импортирования и загрузки содержимого 102 хранилища ключей в защищенное хранилище 108 ключей в соответствии с вариантом раскрытия настоящего изобретения.

После приема содержимого 102 хранилища ключей от провайдера 104 услуг предоставления ключей зашифрованные данные ключей, содержащиеся в хранилище, импортируются в защищенное хранилище 108 ключей пользовательского устройства 106 в ходе выполнения одной операции.

Следует отметить, что данные ключей могут предоставляться в виде одного списка кодов ключей или в виде множества различных списков кодов ключей. Следует принимать во внимание, что различные списки кодов ключей могут импортироваться одновременно. Независимо от формата, в котором зашифрованы различные списки кодов ключей, то есть данные ключей, все данные ключей импортируются в ходе

выполнения одной операции.

Зашифрованные данные ключей затем безопасно дешифруются в хранилище 108 ключей при их загрузке в хранилище 108 ключей.

На фиг. 1A, 1B и 1C представлены лишь примеры, которые не должны неоправданно ограничивать объем приведенной формулы изобретения. Следует понимать, что конкретное назначение системы 100 представлено в качестве примера и не должно толковаться в качестве ограничения системы 100 конкретными числовыми параметрами, типами или структурами поставщиков услуг и пользовательских устройств, в частности, одно пользовательское устройство показано только для простоты изложения. Специалисту в этой области техники понятно, каким образом можно реализовать множество изменений, альтернативных вариантов и модификаций вариантов раскрытия настоящего изобретения.

Следует принимать во внимание, что хотя на фиг. 1B и 1C показаны индексы данных ключей, ссылки на ключи не обязательно всегда реализуются с помощью таких индексов. Следует отметить, что в альтернативных реализациях ссылки на ключи могут быть реализованы с использованием смещений, как описано ранее.

На фиг. 2 показан алгоритм выполнения шагов способа защиты использования содержимого хранилища ключей в устройстве конечного пользователя в соответствии с вариантом раскрытия настоящего изобретения. Способ изображен в виде набора шагов в рамках логической блок-схемы, представляющей последовательность шагов, которые могут быть реализованы аппаратно, программно или с помощью комбинации этих средств, таким образом как описано выше.

На шаге 202 содержимое хранилища ключей принимается в данном пользовательском устройстве. На шаге 202 содержимое хранилища ключей включает в свой состав данные ключей, зашифрованные с использованием реквизитов шифрования, совместимых с данным пользовательским устройством. Содержимое хранилища ключей создается поставщиком услуг предоставления ключей и принимается от него в формате, совместимом с данным устройством конечного пользователя.

На шаге 204 зашифрованные данные ключей содержимого хранилища ключей импортируют в защищенное хранилище ключей данного пользовательского устройства в ходе выполнения одной операции. На шаге 204 содержимое хранилища ключей записывается в защищенное хранилище ключей таким образом, чтобы данные ключей не могли быть экспортированы из хранилища ключей.

На шаге 206 внутренне, в защищенном хранилище ключей данного пользовательского устройства одной или более интегрированным услугам хранилища ключей данного пользовательского устройства предоставляется доступ к неэкспортируемым данным ключей для использования только посредством ссылок на ключи. Как указывалось выше, такие интегрированные услуги предоставляются исполняемым программным обеспечением, которое защищено на уровне ядра, например структуры ядра данного пользовательского устройства. Опционально, структура ядра включает в свой состав аппаратное обеспечение для достижения повышенного уровня безопасности.

Шаги 202 206 показаны только для иллюстрации, также могут быть реализованы альтернативные варианты, в которых добавляются один или более шагов без нарушения объема представленной формулы изобретения.

Возможны изменения в вариантах раскрытия настоящего изобретения, описанных выше, в объеме настоящего изобретения, определенного прилагаемой формулой изобретения. Такие термины, как "включающий", "содержащий", "встроенный", "состоящий из", "имеющий", "представляет собой", используемые в описании и формуле

настоящего изобретения, не должны толковаться как исключающие использование блоков, компонентов или элементов, явно не описанных выше. Ссылка на компонент, указанный в единственном числе, также должна допускать толкование, связанное со множеством компонентов; например, "по меньшей мере один" в одном из примеров указывает на один компонент, а в другом - на множество компонентов; кроме того, конструкция "два из" и подобная ей конструкция "один или более" должны толковаться таким же образом. Числовые значения, заключенные в скобки в прилагающейся формуле изобретения, помогают разобраться в пунктах формулы изобретения и не должны трактоваться в качестве ограничения изобретения, заявленного посредством этой формулы.

Фразы "в варианте осуществления", "согласно варианту осуществления" и т.п.обычно означают, что следующий за фразой конкретный признак, структура или характеристика включается по меньшей мере в один вариант раскрытия настоящего изобретения, а также может включаться в несколько вариантов раскрытия. Важно отметить, что такие фразы не обязательно относятся к одному варианту осуществления.

ССЫЛОЧНЫЕ МАТЕРИАЛЫ

[1] Trusted execution environment (доверенная среда выполнения) - Wikipedia, свободная энциклопедия (дата просмотра: 28 ноября 2016 г.); URL: https://en.wikipedia.org/wiki/Trusted execution environment

[2] Advanced Encryption Standard (улучшенный стандарт шифрования) -Wikipedia, свободная энциклопедия (дата просмотра: 28 ноября, 2016 г.); URL: https://en.wikipedia.org/wiki/Advanced Encryption Standard

(57) Формула изобретения

1. Способ защиты использования содержимого (102) хранилища ключей в пользовательском устройстве (106) конечного пользователя, включающий следующие шаги:

(i) прием, в данном пользовательском устройстве (106), содержимого (102) хранилища ключей, включающего данные ключей, зашифрованные с использованием реквизитов шифрования, совместимых с данным пользовательским устройством (106), при этом содержимое (102) хранилища ключей создано поставщиком (104) услуг предоставления ключей и его принимают от поставщика услуг предоставления ключей в формате, совместимом с данным пользовательским устройством (106), причем данные ключей предоставляют как список кодов ключей;

(ii) импортирование зашифрованных данных ключей содержимого (102) хранилища ключей в защищенное хранилище (108) ключей данного пользовательского устройства и сохранение данных ключей в защищенном хранилище (108) ключей в зашифрованном виде, при этом все зашифрованные данные ключей содержимого (102) хранилища ключей импортируют в ходе выполнения одной операции, и содержимое (102) хранилища ключей сохраняют в хранилище ключей так, что данные ключей не могут быть экспортированы из хранилища ключей, причем упомянутое импортирование содержит: дешифрование зашифрованных данных ключей для получения списка кодов ключей и генерирование ключей путем выбора ключей из списка кодов ключей на основании смещений ключей, смещений байтов и/или смещений битов; и

(iii) внутренне, в защищенном хранилище (108) ключей данного пользовательского устройства (106), предоставление, одной или более интегрированным услугам хранилища ключей данного пользовательского устройства (106), доступа к неэкспортируемым данным ключей для использования только посредством ссылок на ключи.

2. Способ по п. 1, отличающийся тем, что на шаге (ii) содержимое (102) хранилища ключей импортируют в виде одного файла данных.

3. Способ по п. 1 или 2, включающий прием, в содержимом (102) хранилища ключей, индексов, используемых для ссылки на данные ключей посредством ссылок на ключи.

4. Способ по п. 1 или 2, включающий генерацию, в данном пользовательском устройстве (106), индексов, используемых для ссылки на данные ключей посредством ссылок на ключи.

5. Способ по любому из пп. 1–4, отличающийся тем, что хранилище ключей реализовано аппаратно и импортирование на шаге (ii) включает связывание данных ключей, содержащихся в аппаратном хранилище ключей, с защищенной областью аппаратных средств обработки данного пользовательского устройства (106).

6. Способ по любому из пп. 1–5, отличающийся тем, что он включает интеграцию, с хранилищем ключей, одного или более доверенных программных приложений (122) или процессов экосистемы, выполняющихся в данном пользовательском устройстве (106) и авторизованных для использования хранилища ключей данного пользовательского устройства (106).

7. Способ по п. 6, отличающийся тем, что он включает импортирование, от поставщика (120) услуг предоставления доверенного программного обеспечения, одного или более доверенных программных приложений (122) для предоставления интегрированных услуг хранилища ключей, при этом одно или более доверенных программных приложений (122) при выполнении в данном пользовательском устройстве (106) способны предоставлять одну или более интегрированных услуг хранилища ключей и защищены на уровне ядра (124) данного пользовательского устройства (106).

8. Способ по любому из пп. 1–7, отличающийся тем, что он включает защиту хранилища ключей в данном пользовательском устройстве с использованием биологического идентификационного удостоверения конечного пользователя.

9. Способ по любому из пп. 1–8, отличающийся тем, что на шаге (i) данные ключей принимают в данном пользовательском устройстве (106) в форме симметричного шифрования.

10. Способ по любому из пп. 1–9, отличающийся тем, что данные ключей включают по меньшей мере одно из следующего:

(a) секретные ключи для симметричного шифрования данных,

(b) личные ключи и открытые ключи для использования в инфраструктуре, эквивалентной инфраструктуре открытых ключей (PKI),

(c) сертификаты, используемые для криптографии, подписания, обеспечения целостности, верификации, аутентификации, авторизации,

(d) один или более генераторов ключей для генерации ключей.

11. Компьютерное программное изделие, содержащее машиночитаемый носитель информации, на котором хранятся машиночитаемые инструкции, исполняемые вычислительным устройством, в состав которого входят аппаратные средства обработки, для выполнения способа по любому из пп. 1-10.

12. Система (100) для защиты использования содержимого (102) хранилища ключей в пользовательском устройстве (106) конечного пользователя, способная выполнять следующие операции:

(i) прием, в данном пользовательском устройстве (106), содержимого (102) хранилища ключей, включающего данные ключей, зашифрованные с использованием реквизитов шифрования, совместимых с данным пользовательским устройством (106), при этом содержимое (102) хранилища ключей создается поставщиком (104) услуг предоставления

ключей и принимается от поставщика услуг предоставления ключей в формате, совместимом с данным пользовательским устройством (106), причем данные ключей предоставляют как список кодов ключей;

(ii) импортирование зашифрованных данных ключей содержимого (102) хранилища ключей в защищенное хранилище (108) ключей данного пользовательского устройства (106) и сохранение данных ключей в защищенном хранилище (108) ключей в зашифрованном виде, при этом все зашифрованные данные ключей содержимого хранилища (102) ключей импортируются в ходе выполнения одной операции, и содержимое хранилища ключей сохраняется в хранилище ключей так, что данные ключей не могут быть экспортированы из хранилища ключей, причем упомянутое импортирование содержит:

дешифрование зашифрованных данных ключей для получения списка кодов ключей и генерирование ключей путем выбора ключей из списка кодов ключей на основании смещений ключей, смещений байтов и/или смещений битов; и

(iii) внутренне, в защищенном хранилище (108) ключей данного пользовательского устройства (106), предоставление, одной или более интегрированным услугам хранилища ключей данного пользовательского устройства (106), доступа к неэкспортируемым данным ключей для использования только посредством ссылок на ключи.

13. Система по п. 12, отличающаяся тем, что она способна выполнять прием, в содержимом (102) хранилища ключей, индексов, используемых для ссылки на данные ключей посредством ссылок на ключи.

14. Система по п. 12, отличающаяся тем, что она способна выполнять генерацию, в данном пользовательском устройстве (106), индексов, используемых для ссылки на данные ключей посредством ссылок на ключи.

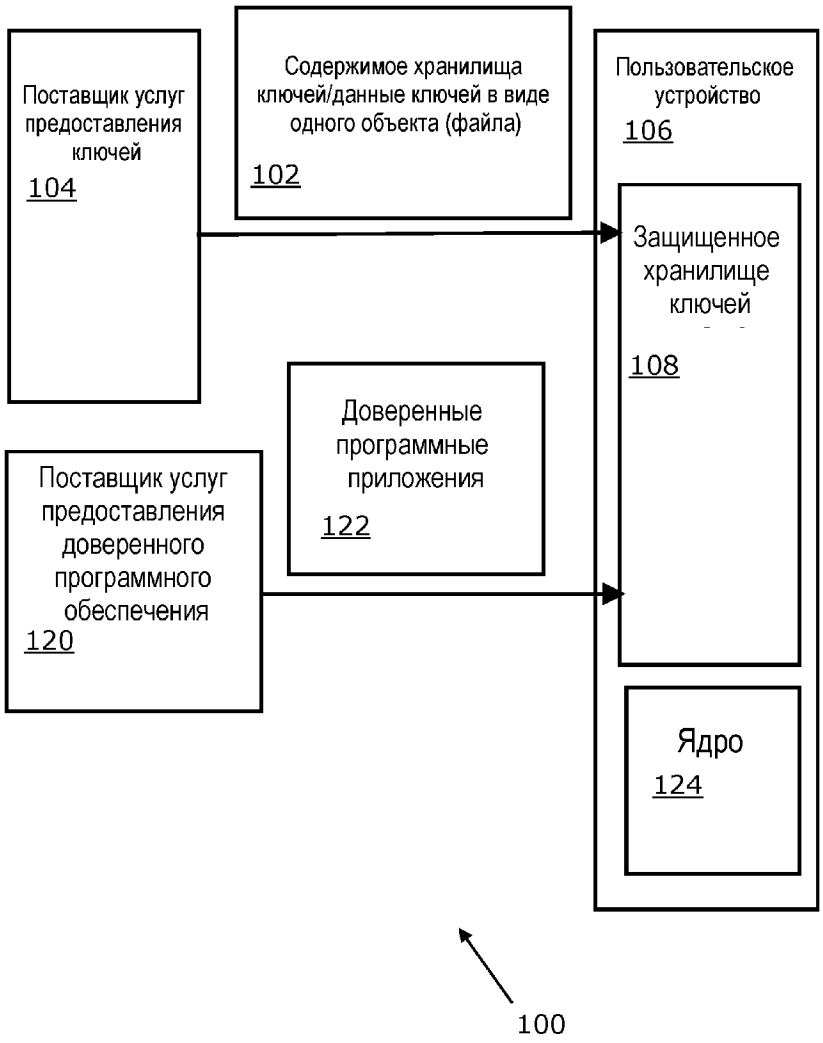
15. Система по любому из пп. 12–14, отличающаяся тем, что хранилище ключей реализовано аппаратно и при импортировании на шаге (ii) система (100) способна выполнять связывание данных ключей, содержащихся в аппаратном хранилище ключей, с защищенной областью аппаратных средств обработки данного пользовательского устройства (106).

16. Система по любому из пп. 12–15, отличающаяся тем, что она способна выполнять интеграцию, с хранилищем ключей, одного или более доверенных программных приложений (122) или процессов экосистемы, выполняющихся в данном пользовательском устройстве (106) и авторизованных для использования хранилища ключей данного пользовательского устройства (106).

17. Система по п. 16, отличающаяся тем, что она способна выполнять импортирование, от поставщика (120) услуг предоставления доверенного программного обеспечения, одного или более доверенных программных приложений (122) для предоставления интегрированных услуг хранилища ключей, при этом одно или более доверенных программных приложений (122) при выполнении в данном пользовательском устройстве (106) способны предоставлять одну или более интегрированных услуг хранилища ключей и защищены на уровне ядра (124) данного пользовательского устройства (106).

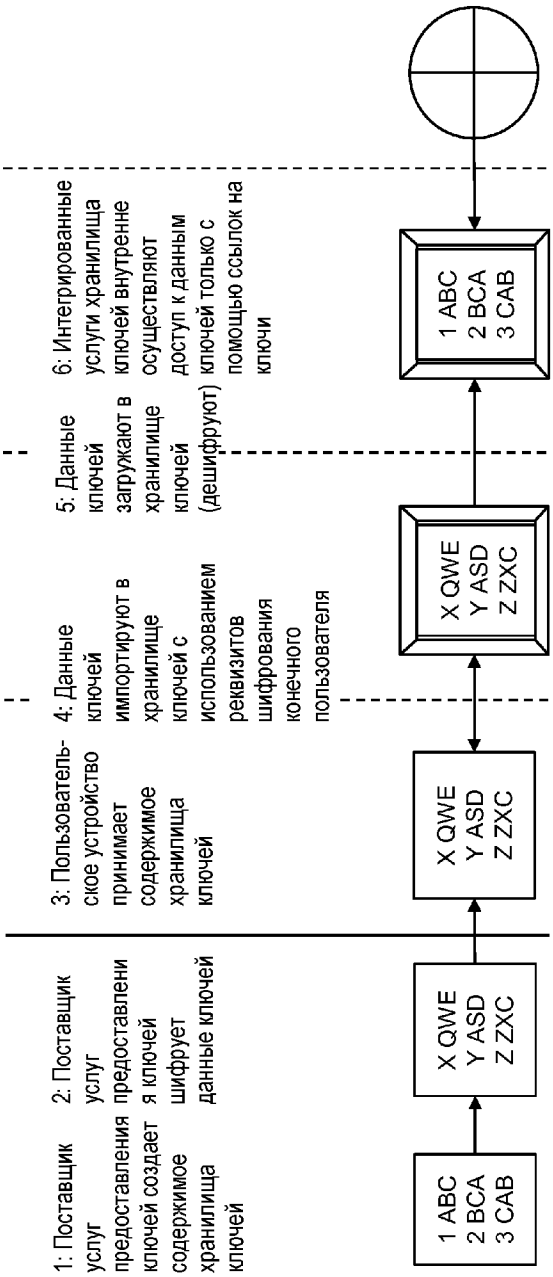
18. Система по любому из пп. 12–17, отличающаяся тем, что хранилище ключей защищено в данном пользовательском устройстве (106) с использованием биологического идентификационного удостоверения конечного пользователя.

1

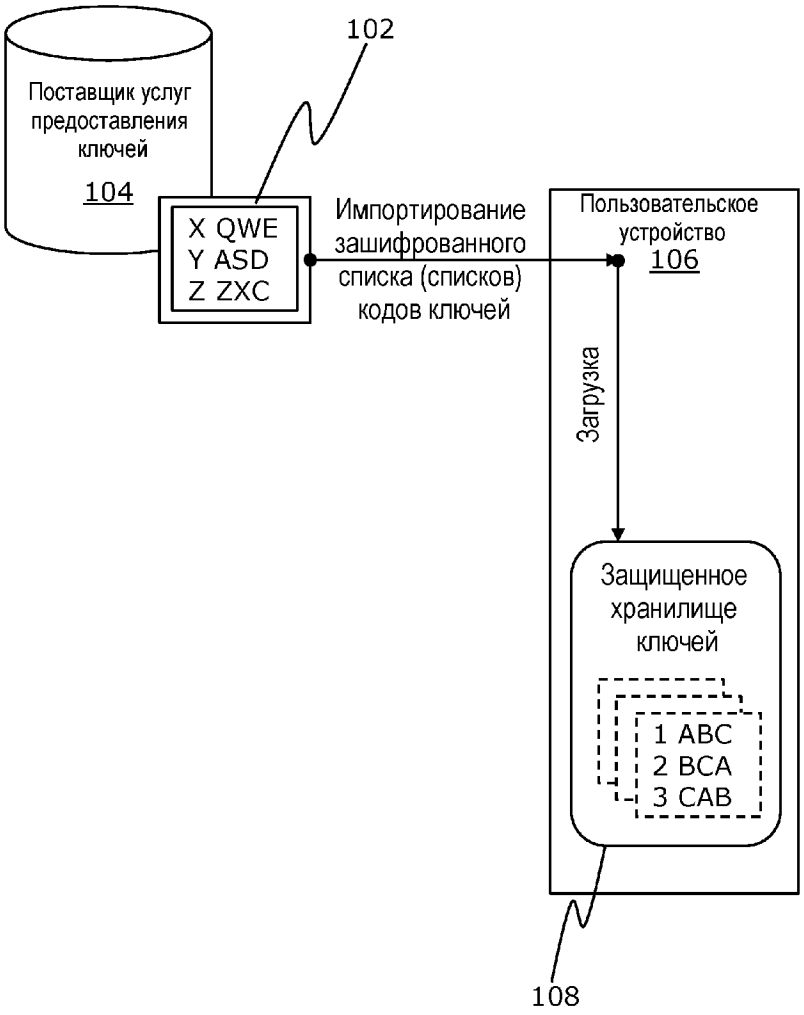

Поставщик услуг предоставления ключей
104
Содержимое хранилища ключей/данные ключей в виде одного объекта (файла)
102
Пользовательское устройство
106
Защищенное хранилище ключей
108
Доверенные программные приложения
122
Поставщик услуг предоставления доверенного программного обеспечения
120
Ядро
124
100

ФИГ. 1А

2


1: Поставщик услуг предоставления ключей создает содержимое хранилища ключей
2: Поставщик услуг предоставления ключей шифрует данные ключей
3: Пользовательское устройство принимает содержимое хранилища ключей
4: Данные ключей импортируют в хранилище ключей с использованием реквизитов шифрования конечного пользователя
5: Данные ключей загружают в хранилище ключей (дешифруют)
6: Интегрированные услуги хранилища ключей внутренне осуществляют доступ к данным ключей только с помощью ссылок на ключи
1 ABC
2 BCA
3 CAB
X QWE
Y ASD
Z ZXC
X QWE
Y ASD
Z ZXC
1 ABC
2 BCA
3 CAB

ФИГ. 1В


102
Поставщик услуг предоставления ключей
104
X QWE
Y ASD
Z ZXC
Импортирование зашифрованного списка (списков) кодов ключей
Пользовательское устройство
106
Загрузка
Защищенное хранилище ключей
1 ABC
2 BCA
3 CAB
108

ФИГ. 1C

4


Прием содержимого хранилища ключей, содержащего данные ключей в зашифрованном виде
202
Импортирование и сохранение зашифрованных данных ключей в защищенном хранилище ключей пользовательского устройства в зашифрованном виде
204
Предоставление интегрированным услугам хранилища ключей доступа к неэкспортируемым данным ключей для использования только с помощью ссылок на ключи
206

ФИГ. 2